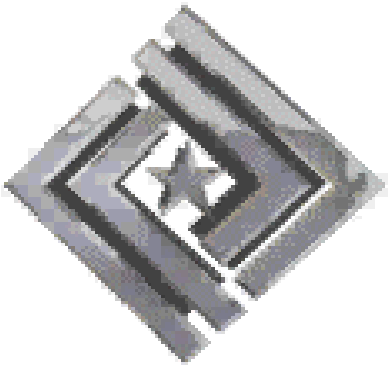


U.S. DEPARTMENT OF LABOR
Office of the Chief Information Officer

SYSTEMS DEVELOPMENT AND LIFE CYCLE MANAGEMENT MANUAL

VERSION 2.0

(FINAL)

WASHINGTON, D.C.
JULY 2000

Systems Development and Life Cycle Management Manual

Table of Contents

LIST OF APPENDICES

Systems Development and Life Cycle Management (SDLCM)

Executive Summary

Annually the U.S. Department of Labor (DOL) invests millions of dollars on information technology (IT) systems. These IT systems are vital to DOL mission programs and administrative functions. The goal is to rely on systems and technology for a safe, secure, and a dependable method to provide services, develop products, administer daily activities, and perform short- and long-term management functions. DOL must ensure data privacy and security when developing and implementing information systems as well as establish uniform privacy and protection practices.

To effectively manage the Department's IT development and maintenance efforts within the framework provided by the "DOL Guide to IT Capital Investment Management (Version 2.0, May 2000)," the DOL developed the Systems Development and Life Cycle Management (SDLCM) Manual. The SDLCM serves as the mechanism to assure that developing, modifying, or enhancing systems meet established user requirements and support DOL critical success factors. It sets forth a standard and logical process for managing IT system development activities and acquisition approvals that are controlled, measured, documented, and ultimately improved while responding to the following current legislation mandating the use of industry standards:

- National Technology Transfer and Advancement Act of 1995
- Information Technology Management Reform Act of 1996 – ITMRA (Clinger-Cohen Act)
- OMB Director's Policy Memorandum M-97-02 (Raines Rules)
- OMB Circulars (e.g., A-130, A-94, A-109)

The SDLCM represents many years of systems development and engineering experience by information systems professionals and the incorporation of lessons learned from prior implementations. The purpose of this manual is to disseminate proven practices for use throughout the DOL. The specific benefits expected include the following:

- Reduced risk of IT system project failure.
- Consideration of DOL program environments and associated system and data requirements throughout the entire life of the system (lessons learned).
- Early identification of technical and management issues to avoid investments in features or functions not benefiting the business community.
- Formalization of the IT system acquisition approval process.
- Disclosure of all life cycle costs to guide business decisions.

- Fostering realistic expectations of what the system will and will not provide, through active user involvement.
- Information to enable consideration of all aspects -- programmatic, technical, management, and cost -- of a proposed system development or modification effort.
- Encouragement of periodic evaluations to identify systems that are no longer effective.
- Measurements of progress and status to enable effective corrective action before proceeding to the next phase.
- Information that supports effective resource management and budget planning.

The DOL's SDLCM divides an IT system's life cycle into seven (7) phases starting with conceptual planning and ending with disposition. It describes the inputs, activities and deliverables associated with each phase. Further, it presents guidance on how the approach can be tailored to suit the various types of systems development and maintenance projects that exist within the DOL today.

The use of the SDLCM applies to all DOL and contractor personnel who are developing, acquiring (e.g., Commercial Off-the-Shelf (COTS)), or managing new systems, or making modifications or enhancements to existing systems. Adherence to the SDLCM by system developers, users, and all levels of DOL management across all functional areas is crucial to delivering cost effective information systems. DOL Agencies are responsible for ensuring that the systems development and management approach described in the SDLCM is practiced on a day-to-day basis. The Chief Information Officer/Office of the Chief Information Officer (CIO/OCIO) is the ultimate authority for the SDLCM.

Systems Development and Life Cycle Management (SDLCM)

1. INTRODUCTION

This manual describes the U.S. Department of Labor's (DOL's) Systems Development and Life Cycle Management (SDLCM) methodology. The SDLCM presents a seven-phase structured approach to developing and managing IT projects from concept to disposition. The concepts presented are the foundation for the life cycle management approach adopted by the DOL to improve the quality of their information technology (IT) systems.

The SDLCM follows the IT development and management framework provided by DOL Guide to IT Capital Investment Management (Version 2.0, May 2000). Exhibit 1-1 shows the processing of IT projects and how they feed into the seven-phase SDLCM approach. Moreover, the exhibit maps the SDLCM to the three phases (Select, Control and Evaluate) of the IT Capital Planning and Investment. Process reviews by Agency, OCIO, Management Review Council (MRC), and the Technical Review Board (TRB) are conducted and recommendations/approvals are given addressing risk, complexity, cost and budget coverage. The products of these organizations help facilitate project success.

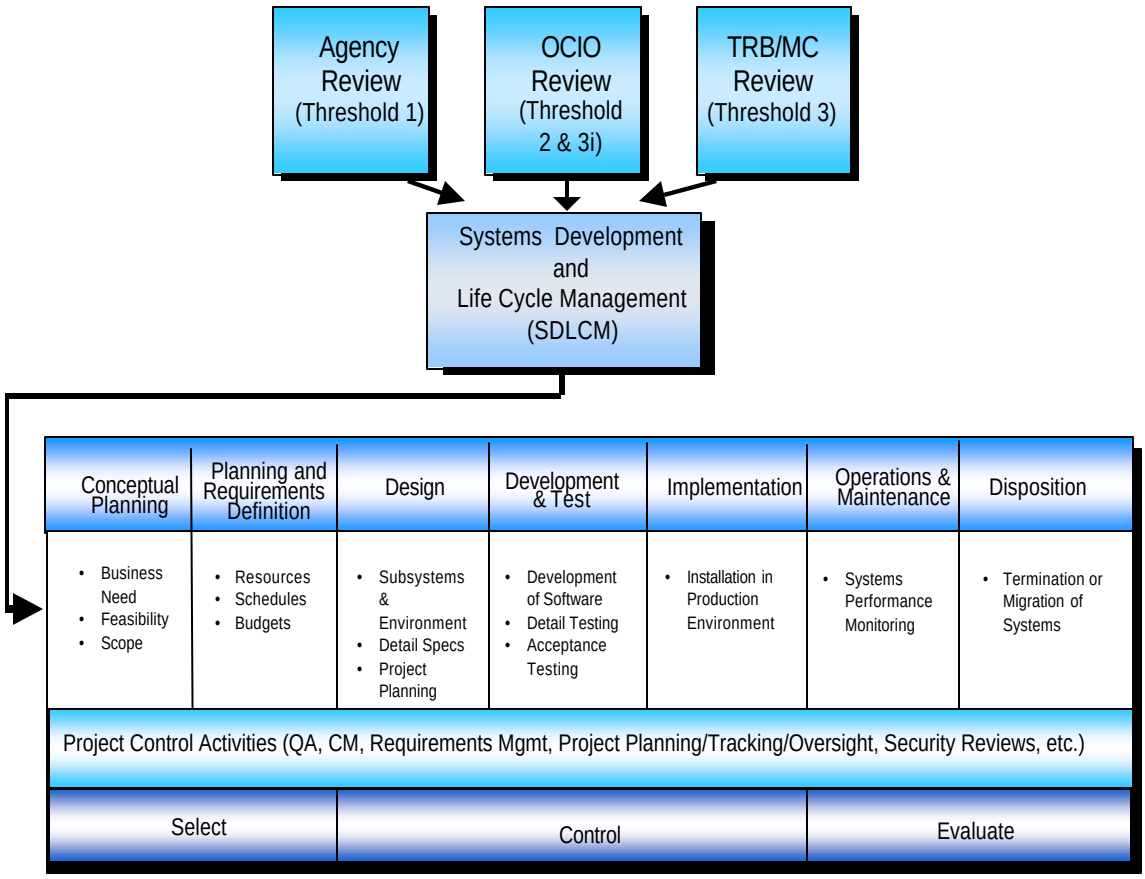
As shown in Exhibit 1-1, there are four thresholds governing approval authority of IT systems. They are defined as follows:

Threshold 1: Initiatives with expected investment costs up to $100,000 annually. Initiatives meeting Threshold 1 criteria are self-certified at the Agency-level per the format listed in the DOL Guide to IT Capital Investment Management (i.e., DOL Guide)

Threshold 2: Initiatives with expected investment costs between $100,000 and $5,000,000 annually. Threshold 2 initiatives are entered into the Information Technology Investment Portfolio System (I-TIPS) and reviewed for approval by the OCIO using the procedures found in the DOL Guide. I-TIPS is an innovative web-based decision support and project management tool for managing IT investments. Additional information on I-TIPS can be found at I-TIPS Online-**http//www.itips.gov.**

Information Technology Capital Planning and Investment Phases

Exhibit 1-1: DOL Systems Development and Life Cycle Management (SDLCM) Methodology



Threshold 3i: Initiatives that involve modification/revisions to the existing IT infrastructure with no new technology involved. Review and approval is by OCIO. The TRB is informed at their scheduled meeting of OCIO review decisions.

Threshold 3: All initiatives above $5,000,000 annual investment costs and any initiative, regardless of dollar value, meeting the exception criteria (interoperable, cross-cutting, designated as "high interest," infrastructure related, or affecting financial systems or data) will be entered into I-TIPS. Then these initiatives will be reviewed by the TRB with corresponding referrals to the DOL Management Review Council (MRC) per the procedures found in the DOL Guide.

Chapter 1 of this manual provides an introduction to the DOL SDLCM including organization of the document, an overview of the SDLCM phase activities, a description of supporting project management activities; and a description of the roles and responsibilities of key organizations involved in the SDLCM. Chapter 2 discusses how the SDLCM can be applied across the various types of projects within the DOL; four work patterns are described. Chapters 3 through 9 describe the full-sequential life cycle methodology from the Conceptual Planning Phase through the Disposition Phase. A glossary and acronym list is provided in Appendix A. Appendices B through G contain reference material and general guidance for preparing deliverables for each of

the seven phases of the SDLCM. Appendix H contains an in depth matrix for the SDLCM with references to governing policy and associated industry standards cited.

1.1 Strategic Planning

Strategic planning affects SDLCM application systems projects by assessing the benefits that each project will provide and how these benefits support the DOL Strategic Plan. The purpose is to ensure that all IT systems development life cycle activities support DOL's strategic goals. Strategic planning is not part of the SDLCM, but it determines what information systems projects are to be initiated and will continue to receive funding. A description of the strategic planning process is outside the scope of the SDLCM; however, there are several important activities that affect a project's life cycle. They are described below.

1.1.1 Strategic Management Process

The aim of the strategic management process is to identify potential improvements to DOL information systems and to gain commitment of the required resources to change these systems. This process develops and revises the Information Resources Management (IRM) Strategic Plan based on the priorities defined in the DOL Strategic Plan. This strategic management process ensures that effective plans are deployed and that the "return on investment" is an essential measure of performance. It enables each individual application systems project to develop detailed plans that support the overall DOL effort, while solving project-specific problems. DOL has defined the strategic management process in the "Information Technology Architecture, Phase I: Mission Critical Baseline Characterization and Opportunity Assessment, March 16, 2000."

1.1.2 Business Process Reengineering

Business process reengineering (BPR) is performed to change the way an organization conducts its business. BPR is the redesign of the organization, culture, and its business processes to achieve significant improvements in costs, time, service, and quality. It complements and augments the strategic management process, and may result in the initiation of an application systems project(s). BPR is performed before initiation of an application systems project.

1.1.3 Performance Measurement

Performance measurement is an essential element in developing effective systems through a strategic management process. The mission, goals, and objectives of DOL are identified in its strategic plan. Strategies are developed to identify how DOL can achieve the goals. For each goal, DOL establishes a set of performance measures. These measures of performance enable DOL to assess how effective each of its projects is in improving DOL operations. They also address compliance with OMB Circular A-94, which states the following guidelines:

- Plan for periodic results-oriented evaluations of program effectiveness using the quantified measures developed in the economic analysis.

- Place a high priority on information systems projects whose benefits accrue to the public or to other levels of Government

- Understand that funding approval request of most information system projects is based on a reasonable tradeoff between using the funds for the information system and using the funds for other program objectives.

1.2 SDLCM Roles and Responsibilities

During the Conceptual Planning Phase, the Project Manager and appropriate project team members are identified. An individual, team, or reviewing authority such as the sponsoring agency, OCIO, TRB or MRC, as appropriate, is designated as having review and approval responsibility for project milestones and products prior to the project continuing to the next phase. Other organizations and individuals become actively involved in the life cycle as the IT system matures. These organizations include user organizations or individuals responsible for database management, data administration, Configuration Management (CM), acquisition (procurement) support, and system security. Responsibilities and roles of important organizations involved throughout the systems development and management life cycle are described below.

1.2.1 Management Review Council (MRC)

Management Review Council (MRC) is chaired by the Deputy Secretary. The MRC has the following responsibilities:

- "Evaluate and either approve, not approve, or approve with conditions TRB recommendations on IT portfolios and initiatives and advise the CIO of the results." (Secretary's Order 1-2000, "Authority and Responsibilities for Implementation of the Paperwork Reduction Act of 1995 (P. L. 104-13) and the Clinger-Cohen Act of 1996 Information Technology Management Reform Act of 1996) (Division E of P. L. 104-106)," Section 8, b, 1, page 9.)

- "Ensure that MRC decisions and recommendations pertaining to IT investments management deliver substantial business benefit to the Department and/or substantial return-on-investment to the taxpayer." (Secretary's Order 1-2000, "Authority and Responsibilities for Implementation of the Paperwork Reduction Act of 1995 (P. L. 104-13) and the Clinger-Cohen Act of 1996 Information Technology Management Reform Act of 1996) (Division E of P. L. 104-106)," Section 8, b, 2, page 9.)

1.2.2 Technical Review Board (TRB)

The Technical Review Board (TRB) serves as the Department's first tier investment review board

for above threshold information technology (IT) investments and as a forum to identify and resolve Department-wide IT-related issues. The TRB makes recommendations on the appropriate disposition of above threshold IT investments to the MRC based on standardized investment review criteria, with a focus on the technical feasibility of the investments. The TRB also serves as a forum to conduct Departmental IT strategic planning, IT architecture management, and IT capital planning process improvements. The Deputy CIO chairs the TRB. (Secretary's Order 1-2000, "Authority and Responsibilities for Implementation of the Paperwork Reduction Act of 1995 [P. L. 104-13] and the Clinger-Cohen Act of 1996 Information Technology Management Reform Act of 1996) (Division E of P. L. 104-106), (Technical Review Board Charter)

1.2.3 Chief Information Officer (CIO)/Office of the Chief Information Officer (OCIO)

The Information Technology Management Reform Act (ITMRA) amended the Paperwork Reduction Act (PRA) to: a) create the position of Department CIO, and b) assign all PRA duties previously assigned to Department "senior officials" to a Department CIO.

The Secretary's Order (1-2000) Authority and Responsibilities for Implementation of the Paperwork Reduction Act of 1995 (P. L. 104-13) and the Clinger-Cohen Act of 1996 (Information Technology Management Reform Act of 1996) (Division E of P. L. 104-106) delegates authority and assigns responsibility for implementation of the Paperwork Reduction Act of 1995 (P. L.104-13) and the Information Technology Management Reform Act (ITMRA) of 1996 (Division E of P. L.104-106) and formally establishes within the Department of Labor the position of the Chief Information Officer (CIO). The Secretary's Order (1-2000) states that the CIO provides advice and other assistance to the Secretary of Labor and other senior management personnel of the DOL to ensure that information technology (IT) is acquired and information resources are managed for the Department in a manner that implements the policies and procedures of the ITMRA. In accordance with the duties assigned to the CIO by the ITMRA, the CIO:

- Serves as the senior IT advisor to the Secretary and the Management Council.
- Is responsible for presenting proposed IT portfolios.
- Promotes the effective and efficient design and operation of all major information management processes for the Department and provides final portfolio enhancement.
- Designs, implements and maintains in the DOL a process for maximizing the value and managing the risks of the IT acquisitions. By providing a means for senior management personnel to obtain timely information regarding the progress of an investment in an information system, including a system of milestones for measuring progress, on an independently verifiable basis, in terms of cost, capability of the system to meet specified requirements, timeliness, and quality.

The Management Review Council (MRC) shall designate the Deputy CIO to chair, and manage a Technical Review Board (TRB). The TRB assists the CIO with IT capital investment management, budgeting, architecture development, and critical infrastructure protection, and participates in other DOL IT management activities as requested by the CIO.

The TRB serves as the Department's first tier Investment Review Board for above threshold IT investments. In that context of this document, the role of the OCIO can be summarized below with respect to the four thresholds of IT investment established in the IT Capital Planning Guidance:

- Threshold 1 of IT Capital Planning Guidance - Agency Level Review and Approval. The OCIO does not review individual initiatives at this level; it is an Agency responsibility. The OCIO is responsible for providing periodic oversight of the Agencies management of IT. In particular, the OCIO is required to ensure that the Agency complies with the guidance provided in this System Development and Life Cycle Management (SDLCM) Manual.

- Threshold 2 of the IT Capital Planning Guidance - OCIO Level Review and Approval. The OCIO is the review and approval authority for individual IT initiatives at this level. The OCIO will review the initiative to ensure that the project complies with the guidance provided in the SDLCM. This includes ensuring the supporting documentation for the initiatives have been negotiated between the OCIO and the Agency.

- Threshold 3i of the IT Capital Planning Guidance - OCIO Level Review and Approval. The OCIO is the review and approval authority for individual IT initiatives at this level. Initiatives that involve modification/revisions to the existing IT infrastructure with no new technology involved. The OCIO shall keep the TRB informed at their scheduled meeting of its reviews and approvals.

- Threshold 3 of the IT Capital Planning Guidance – Technical Review Board (TRB)/Management Review Council (MRC) Level Review and Approval. The TRB/MRC are the review and approval authority for individual IT initiatives at this level. The OCIO will assist the TRB/MRC by reviewing the initiative to ensure that the project complies with the guidance provided in the SDLCM. This includes ensuring that any additional requirements of the TRB/MRC have been followed by the initiating project. If in compliance, the OCIO recommends support of the initiative to the TRB/MRC.

1.2.4 Agency Head

As stated in the Secretary's Order 1-2000**,** roles and responsibilities of the Agency Head are as follows:

- All Agency Heads are assigned responsibility to fully support the CIO in matters concerning

information collection and burden reduction and to ensure compliance by their organizations with CIO, OMB, and PRA guidance and policies.

- All Agency Heads are assigned responsibility to fully support the TRB and MRC in matters pertaining to IT initiatives and to ensure compliance by their organizations with Clinger-Cohen and DOL IT guidance and policies.

- All Agency Heads are assigned responsibility to fully support the Department-wide initiatives approved by the MRC and sponsored by the CIO, re-engineer agencies' mission related processes to maximize return on IT expenditures, and ensure that IT initiatives are managed for successful implementation.

- The Solicitor of Labor is responsible for providing legal assistance and advice to all officials of the Department who are responsible for activities under PRA and the Clinger-Cohen Act and under this Order, except as provided in Secretary's Order 2-90 (January 31, 1990) with respect to the Office of the Inspector General.

1.2.5 Project Manager

The Project Manager has overall responsibility for coordinating the management and technical aspects of the life cycle of a system, including activities related to the development of a system. Responsibilities of a Project Manager may include (but are not limited to) the following: developing a Project Management Plan; completing a project within schedule, budget and meeting customer needs. In addition, a Project Manager may be responsible for coordinating the development, implementation, operation and maintenance of a system with appropriate units within an agency (including centralized IT staff such as network operations staff, security personnel, database management staff, the IRM manager, etc.) as well as reporting the results of projects to the System Owner and other appropriate agency staff. When appropriate a Project Manager will arrange through agency representatives and the System Owner to have the progress of critical projects presented to the Office of the Chief Information Officer (OCIO), the Technical Review Board (TRB), or another entity within the Capital planning and investment management program. The Project Manager may perform the following functions:

- Determines project team organization based on user and information systems organization recommendations.

- Provides detailed work assignments, making sure there are written tasks for all work.

- Develops measurement criteria that defines acceptable performance of each task.

- Coordinates and/or performs system planning, design, and implementation.

- Schedules and directs SDLCM documentation and milestone reviews and participates in reviews conducted by independent staff or a review committee.
- Leads the resolution of problems during all phases.
- Ensures delivery of base lined and fully documented deliverables required to initiate system implementation.
- Oversees preparation of required documentation and maintains a project file.
- Follows SDLCM guidance as outlined in this manual.
- Coordinates with the Computer Security Officer (CSO) to ensure all security activities are completed. The DOL Computer Security Handbook contains more in-depth information on this subject.

1.2.6 System Owner

The System Owner is located within the DOL organization benefiting from or requesting the work on a systems project and is frequently thought of as the "customer" for that project. The System Owner performs the following functions:

- Maintains active senior-level involvement throughout the development of the system.
- Initiates the need identification process to generate a request for a new information system or modification to an existing system.
- Participates in project review activities and reviews project deliverables.
- Coordinates activities with the Agency IRM/IT manager.
- Obtains and manages the budget throughout the project's life cycle.
- Identifies high-level business functions and the need for new development.
- Defines the scope and context of the new development.
- Selects functional organization representatives as the essential participants on the project team with responsibility for defining functional and user needs.
- Holds review and approval authority for ensuring that developed products meet user requirements.

- The System Owner is responsible for conducting a review of Privacy Act issues to determine applicability. If determined to be appropriate, the System Owner will prepare or oversee preparation of the Privacy Act Notice and coordinate with the Records Management representative on the Privacy Act System Notice.

1.2.7 Users

Active user participation is essential at all levels in the definition, design, and development of an IT system. Users are responsible for initiating and expeditiously resolving issues relating to both system development efforts and identification and documentation of requirements. Specifically, user objectives are as follows:

- Provide a quick and consistent review of the requirements.
- Provide statistical information relative to the work processes.
- Develop performance standards.
- Review and refine the functional requirements and their documentation.
- Approve and prioritize requirements.
- Perform user acceptance testing.

1.2.8 Project Team

Project team members bring technical and functional expertise to the project with each member planning and performing tasks in that individual's area of expertise. Team members may not necessarily serve on the project team for the duration of the project; however, all essential project team members must be identified in the Conceptual Planning Phase of the project.

The project team may include individuals fulfilling the roles of: system developer; system tester; data administrator; database administrator; quality assurance (QA) representative; Computer Security Officer (CSO); Configuration Management (CM) representative; telecommunications representative; Acquisitions Management representative; Systems Operations representative; Freedom of Information Act/Privacy Act (FOIA/PA) representative; and other representatives required by the project. Not every project will have full-time staff assigned to every role, and some projects may not need all roles fulfilled. However, consider all roles during project planning.

1.3 SDLCM Phase Overview

The life cycle review process ensures that all products created during the life cycle meet functional and performance requirements as outlined in all requirements documentation. The requirements for holding specific milestone reviews are determined by the system size, complexity and by management direction. The completion of a phase represents a logical point at which a milestone review should occur.

In formulating a life cycle development process, it is essential that requirements documentation, work efforts and system specifications reflect Department of Labor's guidance on IT Architecture, Security, Capital Planning and Records Management. The specific guidelines are:

- Computer Security Handbook, Version 1.0, April 18, 2000.
- Guide to Capital Investment Management, A Practical Reference for Department and Agency Managers and Staff, Version 2.0, May 2000.
- Information Technology Architecture, Phase I: Mission Critical Baseline Characterization and Opportunity Assessment, March 16, 2000.
- DLMS 1 Records Management, Chapter 400 - Records Management Program.

Decisions reached and deliverables produced in one phase may be updated in subsequent phases. As the project progresses, maintenance of life cycle documentation becomes an integral part of the development process. The SDLCM methodology identifies specific documentation that is prepared or updated during each phase. Some documentation may remain fairly stable and unchanged throughout the life cycle, while others may evolve as the system progresses through the life cycle phases.

Examining the size, scope, and complexity of every project will determine the appropriate work pattern. Depending on specific project requirements, a SDLCM work pattern (see Chapter 2) may be selected that could result in combining or overlapping specific phases and deliverables. An overview of each SDLCM phase follows.

1.3.1 Conceptual Planning Phase

The Systems Development and Life Cycle Management (SDLCM) methodology begins with the Conceptual Planning Phase. It is during this phase that a need to develop or significantly enhance a system is identified, its feasibility and costs assessed, and risk and project-planning approaches defined.

1.3.2 Planning and Requirements Definition Phase

The Planning and Requirements Definition Phase begins after the project has been defined and appropriate resources have been committed. There are two key aspects of this phase: 1) planning and 2) defining the functional requirements that the system will need to address. It is during this phase that the Project Management Plan is updated to include or provide additional detail regarding the development approach and methods, tools, tasks, resources, and schedules. Functional requirements are defined to address data, system performance, security, and maintainability aspects of the system.

1.3.3 Design Phase

Upon completion of the Planning and Requirements Definition Phase, the system progresses to the Design Phase. During this phase, functional requirements are translated into preliminary and detailed designs. Decisions are made to address how the system will meet functional, physical, interface, and data requirements. A preliminary (general) system design emphasizing the functional features of the system is produced as a high level guide. Then a final (detailed) system design is produced which expands the design by specifying all the technical detail needed to develop the system.

1.3.4 Development and Test Phase

During the Development and Test Phase, executable software is developed from detailed design specifications. The system is validated through a sequence of unit, integration, system, and acceptance test activities. The objective is to ensure that the system functions as expected and user requirements are satisfied. Large systems are solicited, awarded, and managed in accordance with the Acquisition Plan. All hardware, system software, communications, applications, procedures, and associated documentation are developed/acquired, tested, and integrated. This phase requires strong user participation in order to verify thorough testing of all requirements and meet all business needs.

1.3.5 Implementation Phase

During the Implementation Phase, the new or enhanced system is installed in the production environment, users are trained, data is converted (as needed), and the system is turned over to the user. This phase includes efforts required to implement the system as well as to resolve any problems identified during the implementation process.

1.3.6 Operations and Maintenance Phase

Once a system becomes operational, it moves to the Operations and Maintenance Phase. The emphasis of this phase is to ensure that the user needs continue to be met and that the system continues to perform according to specifications. Routine hardware and software maintenance and upgrades are performed to ensure effective system operations. User training continues during this phase as needed, to acquaint new users to the system or to introduce new features to the current

users. Additional user support is provided, as an ongoing activity, to help resolve reported problems. This phase continues until the system is retired.

1.3.7 Disposition Phase

The Disposition Phase represents the end of the systems life cycle. It provides for the systematic termination of a system to ensure that vital information is preserved for potential future access and/or reactivation. The system, when placed in the Disposition Phase, has been declared surplus and/or obsolete, and is scheduled to be shut down. The emphasis of this phase is to ensure that the system (e.g. software, data, procedures, and documentation) is packaged and archived in an orderly fashion, enabling the system to be reinstalled later, if desired. System records are retained in accordance with DOL policies regarding retention of electronic records.

1.4 Project Management Overview

In addition to performing day-to-day project management duties described in Section 1.2.5, the Project Manager (PM) must ensure that responsibilities have been assigned (if not already the responsibility of the PM), as needed to address the following areas of project management and control:

- Project Planning - Ensure project work approach, commitments, and estimates of the effort are documented in Project Management Plan (PMP).

- Project Tracking and Oversight - Permit project management team to continually assess and manage risks, identify future resource requirements, and recommend corrective actions.

- Configuration Management (CM) - Protect the baseline system configuration from unauthorized and uncoordinated changes, and control future version releases.

- Quality Assurance (QA) - QA is an independent function that objectively monitors and reports the application of methodology, policies, processes, procedures, and standards that contract and/or project personnel use to develop software products and services and/or hardware deliverables.

- Integrated Data Management - Ensure effective management of all DOL data and adherence to DOL's Information Technology Architecture (ITA) model. All systems are created and maintained in accordance with data management policies and practices. Life cycle activities are to be carried out consistently with the existing and planned data management environment and data management concerns will be addressed during all phases of the life cycle.

1.5 Security Compliance

1.5.1 Telecommunications, Communications, and Information Security Policy Considerations

The CIO is responsible for overseeing the protection of information assets against loss, theft, damage, and unauthorized destruction, modification, and access. To ensure IT system security, various security activities are performed throughout the systems development life cycle. A description of the security activities and documented security procedures can be found in the DOL Computer Security Handbook, Version 1.0 (April 18, 2000). All project planners and project managers should refer to it frequently, when planning and managing system projects.

1.5.2 Agency Point of Contact

The Agency Point of Contact (POC) for security matters is the primary point of contact for computer and telecommunications security for the Agency. The DOL Computer Security Officer (CSO) manages computer and telecommunications security. The CSO is responsible for coordinating program requirements throughout the DOL with designated POCs. All projects will identify, in writing, a POC who is responsible for the following:

- Identification of all security systems at the Agency site in accordance with the Computer Security Act of 1987 and Office of Management and Budget Circular A-130.
- Provision of security summary information.
- Development of security plans for Agency systems under the Computer Security Officer's (CSO) direct management control.
- Ensuring security plans are developed for other Agency systems and assisting in the implementation of the Agency's Computer and Technical Security (C&TS) Program.
- Ensuring that Computer Security Certifications (CSCs) are designated, in writing, for all Agency systems and to assist in the implementation of the Agency C&TS Program.
- Ensuring that all pending procurements include provisions for system security, including reviewing procurements for compliance with system security orders.
- Coordinating with the necessary security office in the event procurements involve other security programs (that is, personnel, classified, physical, communications, and security education).

Systems Development and Life Cycle Management (SDLCM)

2. SDLCM WORK PATTERNS

An important objective of the Systems Development and Life Cycle Management (SDLCM) methodology is to provide flexibility that allows tailoring to suit the characteristics of a particular IT system development. One methodology does not necessarily fit all sizes and types of system development and enhancement efforts. The SDLCM provides this flexibility by providing four work patterns that characterize the various types of projects that exist within the DOL. The full sequential work pattern is the model for all project development processes. The level of detail captured within the documentation is reviewed and determined based on the Capital Planning Threshold Level approval authority. A work pattern permits a project planner to tailor the Project Management Plan to meet the specific needs of the project and still conform to SDLCM standards.

During the Planning and Requirements Definition Phase, the Project Manager and Project Owner or other agency authorities will evaluate the system concept definition documentation and identify the work pattern that best suits the IT development or maintenance effort. The four patterns of work for DOL IT system efforts are as follows:

Large System Effort - Threshold 3 Initiative

Medium New System Effort - Threshold 2 Initiative

Maintenance and Enhancement Effort - Threshold 3i Initiative

Small New System - Threshold 1 Initiative

Commercial-off-the-Shelf Software (COTS) integration and enhancement efforts may be applied to any of the work patterns described above. Existing documentation is adopted where applicable and developing core deliverables according to Agency policy and procedures. A description of each of the four SDLCM work patterns is provided in the following sections.

2.1 Large System Effort Work Pattern

The Large System Effort Work Pattern is also referred to as the "Full-Sequential Work Pattern" and follows the methodology described in Chapters three through nine of this manual. The system effort may be a replacement, modernization, or a new development initiative and is characterized as a Threshold 3 Initiative. Exhibit 2-1 shows the core, optional and updated deliverables for each phase. A detailed deliverables matrix for this work pattern, showing governing regulations and policies as well as associated industry standards, is provided in Appendix H.

	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6	Phase 7
RITS/Statement of Concept	C						
Cost Benefit Analysis	C	U	U				
Risk Management Plan	C	U	U	U	U	U	
Project Management Plan	C	U	U	U	U		
Feasibility Study	O						
Acquisition Strategy/Plan	O	O	C	U	U		
Work Breakdown Structure	O	O	C	U	U		
SOW	O						
Functional Requirements Document		C					
Project Risk Assessment		C	U	U	U	U	
System Security Plan/Security Risk Assessment		C	U	U	U	U	
Test Plans		O	O	C			
CM Plan		O	C	U	U		
Legacy Data Plan		O					
Detailed Design			C				
Contingency Plan			O				
Implementation Plan			O	C			
Acceptance Test Plan				C			
Acceptance Test Report				C			
Acceptance Test Approval				C			
Training Plan				C			
Delivered System				C			
System Manuals				C	U	U	
User Manuals				C	U	U	
System Fielding Authorization				O			
Agency Computer Security Certification					C		
Security Accreditation Letter					C		
Implemented System					C		
Trained Personnel					C		
Implementation Certification Statement					C		
Disposition Plan						C	
Archived System							C

Legend

Phase 1 - Conceptual Planning Phase
Phase 2 - Planning & Requirements Definition Phase
Phase 3 - Design Phase
Phase 4 - Development & Test Phase
Phase 5 - Implementation Phase
Phase 6 - Operations & Maintenance Phase
Phase 7 - Disposition Phase

C - Core
O - Optional
U - Updated

Exhibit 2-1: Large System Effort Work Pattern (Full-Sequential)

2.2 Medium New System Effort Work Pattern

The Medium New System Effort Work Pattern applies to new IT system efforts with a Threshold 2 Initiative level. This work pattern closely follows the Large System Effort Work Pattern. Core deliverables are the same, except the Agency will determine the level of detail and rigor to apply commensurate with the dollar effort of the project. Multiple deliverables may be combined, as appropriate, resulting in fewer documents. Exhibit 2-2 shows the core deliverables for each phase of this work pattern.

	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6	Phase 7
RITS/Statement of Concept	C						
Cost Benefit Analysis	C						
Risk Management Plan	C						
Project Management Plan	C						
Feasibility Study							
Acquisition Strategy/Plan			C				
Work Breakdown Structure			C				
SOW							
Functional Requirements Document		C					
Project Risk Assessment		C					
System Security Plan/Security Risk Assessment		C					
Test Plans				C			
CM Plan			C				
Legacy Data Plan							
Detailed Design			C				
Contingency Plan							
Implementation Plan				C			
Acceptance Test Plan				C			
Acceptance Test Report				C			
Acceptance Test Approval				C			
Training Plan				C			
Delivered System				C			
System Manuals				C			
User Manuals				C			
System Fielding Authorization							
Agency Computer Security Certification					C		
Security Accreditation Letter					C		
Implemented System					C		
Trained Personnel					C		
Implementation Certification Statement					C		
Disposition Plan						C	
Archived System							C

Legend

Phase 1 - Conceptual Planning Phase
Phase 2 - Planning & Requirements Definition Phase
Phase 3 - Design Phase
Phase 4 - Development & Test Phase
Phase 5 - Implementation Phase
Phase 6 - Operations & Maintenance Phase
Phase 7 - Disposition Phase

C - Core
O - Optional
U - Updated

Exhibit 2-2: Medium New System Effort Work Pattern

2.3 Maintenance and Enhancement Effort Work Pattern

The Maintenance and Enhancement Effort Work Pattern applies to existing IT systems that are being maintained or enhanced. This is a Threshold 3i Initiative. Funding for this work pattern may come from the Agency steady-state (base) of operations. Updating existing documentation, as needed. Exhibit 2-3 shows the minimum core deliverables for each phase of this work pattern.

	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6	Phase 7
RITS/Statement of Concept	C						
Cost Benefit Analysis							
Risk Management Plan							
Project Management Plan							
Feasibility Study							
Acquisition Strategy/Plan							
Work Breakdown Structure							
SOW							
Functional Requirements Document		C					
Project Risk Assessment							
System Security Plan/Security Risk Assessment							
Test Plans				C			
CM Plan							
Legacy Data Plan							
Detailed Design							
Contingency Plan							
Implementation Plan				C			
Acceptance Test Plan							
Acceptance Test Report							
Acceptance Test Approval							
Training Plan							
Delivered System				C			
System Manuals							
User Manuals							
System Fielding Authorization							
Agency Computer Security Certification							
Security Accreditation Letter							
Implemented System					C		
Trained Personnel					C		
Implementation Certification Statement					C		
Disposition Plan							
Archived System							

Legend

Phase 1 - Conceptual Planning Phase
Phase 2 - Planning & Requirements Definition Phase
Phase 3 - Design Phase
Phase 4 - Development & Test Phase
Phase 5 - Implementation Phase
Phase 6 - Operations & Maintenance Phase
Phase 7 - Disposition Phase

C - Core
O - Optional
U - Updated

Exhibit 2-3: Maintenance and Enhancement Effort Work Pattern

2.4 Small System Effort

The Small System Effort Work Pattern applies to a new IT system development effort with a Threshold 1 Initiative level. The system effort involves development of or update to deliverables that are relatively minor in nature. Documentation follows the normal policies and procedures established by the Agency. Exhibit 2-4 shows the minimum core deliverables for each phase of this work pattern.

	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6	Phase 7
RITS/Statement of Concept	C						
Cost Benefit Analysis							
Risk Management Plan							
Project Management Plan							
Feasibility Study							
Acquisition Strategy/Plan							
Work Breakdown Structure							
SOW							
Functional Requirements		C					
Project Risk Assessment							
System Security Plan/Security Risk Assessment							
Test Plans/Criteria				C			
CM Plan							
Legacy Data Plan							
Detailed Design							
Contingency Plan							
Implementation Plan							
Acceptance Test Plan							
Acceptance Test Report							
Acceptance Test Approval				C			
Training Plan							
Delivered System/Product				C			
System Manuals							
User Manuals							
System Fielding Authorization							
Agency Computer Security Certification							
Security Accreditation Letter							
Implemented Product/Documentation					C		
Trained Personnel							
Implementation Certification Statement							
Disposition Plan							
Archived System							

Legend

Phase 1 - Conceptual Planning Phase
Phase 2 - Planning & Requirements Definition Phase
Phase 3 - Design Phase
Phase 4 - Development & Test Phase
Phase 5 - Implementation Phase
Phase 6 - Operations & Maintenance Phase
Phase 7 - Disposition Phase

C - Core
O - Optional
U - Updated

Exhibit 2-4: Small System Effort Work Pattern

2.5 Additional Work Patterns

Project teams should endeavor to follow the appropriate work pattern that best applies to their particular project. However, from time to time, new project environments or system requirements may evolve necessitating the definition of a new work pattern. In this situation, the Project Manager will arrange through appropriate agency representatives and the System Owner to coordinate with the designated OCIO representative, to develop and document a proposed new work pattern, submit it as an update to this manual, and use it as the basis of their project planning and execution.

Systems Development and Life Cycle Management (SDLCM)

3. CONCEPTUAL PLANNING PHASE

3.1 Phase Overview

The Systems Development and Life Cycle Management (SDLCM) methodology begins with the Conceptual Planning Phase. It is during this phase that a need to develop or significantly enhance a system is identified, its feasibility and costs assessed, and risk and project-planning approaches defined. Exhibit 3-1 identifies key inputs, activities, and deliverables of this phase.

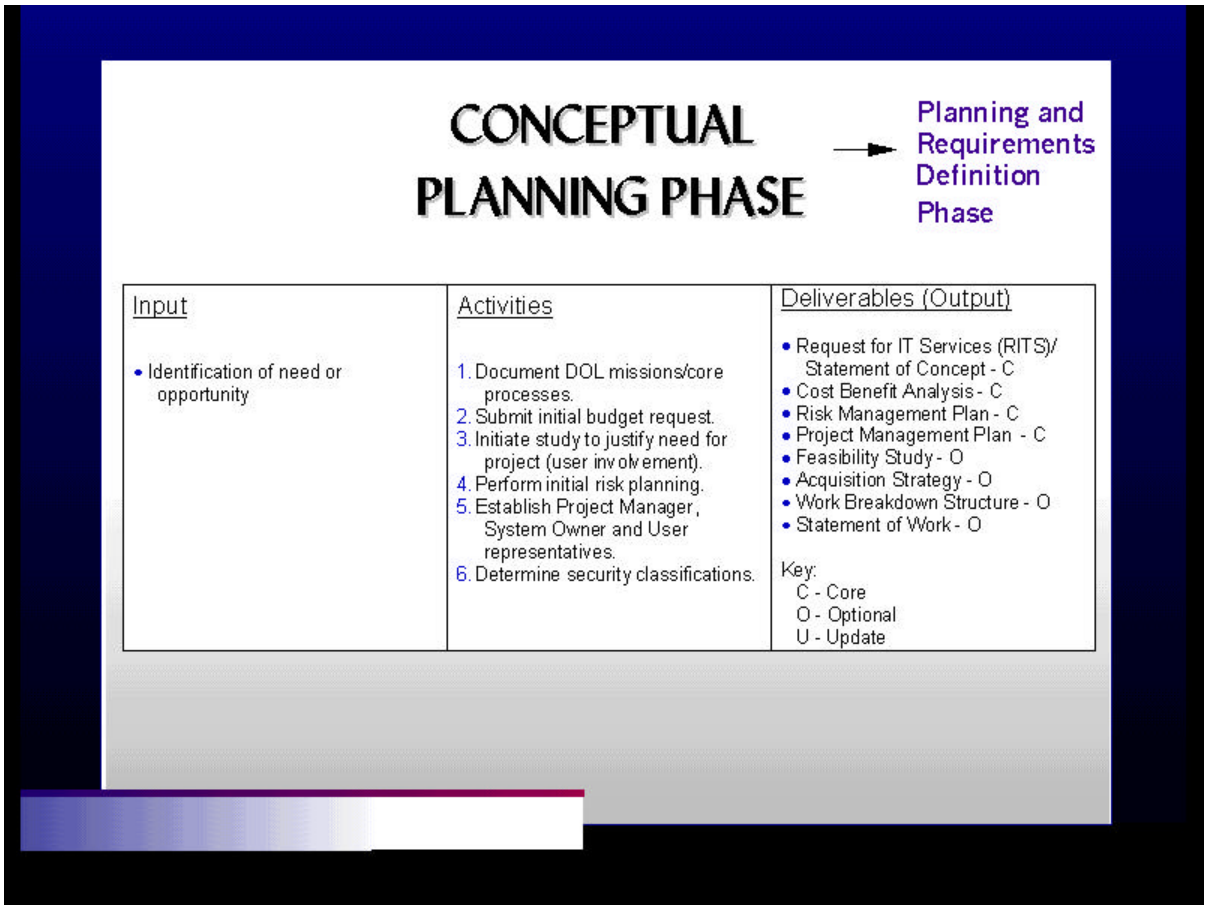


Exhibit 3-1: Conceptual Planning Phase Inputs, Activities, Deliverables

3.2 Phase Inputs

Conceptual planning begins with a need to develop a new IT (information technology) system or to enhance an existing one. The identification for a need or opportunity may be communicated via telephone, e-mail or a verbal discussion.

The Request for Information Technology Services (RITS) may become documented in a statement of work (SOW). Subsequently, justification for continuation occurs at the Agency level, through a Feasibility Study, a Cost Benefit Analysis (CBA), and Risk Management Plan initiates the remaining life cycle phases. Alternately, failure to justify further work results in the appropriate early termination of the project. During the justification process, a functional manager provides the first critical description of the information management concept and secures the resources needed for further examination of the concept and potential approaches.

Ideally, strategic planning and review activities performed prior to the submission of a RITS identify and prioritize business needs or opportunities for systems work. Alternately, to begin the justification process, a functional manager may prepare a concept paper (issue paper or decision paper) that identifies and describes the information management concept. Depending on the sensitivity or criticality of the issue, the functional manager may submit the concept paper to program management or executive management for information and/or approval.

3.3 Phase Activities

3.3.1 Document DOL Mission/Core Processes

A review of DOL's mission statement is critical before initiating an IT project. The following two important points are noted here:

- There is a strong emphasis on defining the information management need or opportunity and linking it to specific U.S. Department of Labor (DOL) missions and/or core processes, as required by the Clinger-Cohen Act, implemented by the Office of Management and Budget (OMB).

- No assumption can be made that the approach will necessarily result in the development of a new system or the replacement of a manual process with an automated system. A modification to existing manual or automated systems may be the best approach to address the need or opportunity; the determination will be recommended in the Feasibility Study. In all cases, a manual process should be evaluated for improvement opportunities before considering automation.

3.3.2 Submit Initial Budget Request

An initial budget request is prepared and submitted to ensure the availability of funding, personnel, and other resources to proceed with subsequent conceptual planning activities of this phase as well as to proceed to the Planning and Requirements Definition Phase.

3.3.3 Initiate Study to Justify Project Need

The Conceptual Planning Phase is where the identification of need is formalized. The need or opportunity identified prior to initiating this phase is formalized into a Request for IT Services (RITS) or Statement of Concept defining what the need is, benefits to the organization, and the proposed solution and approach. The IT system concept is defined in business terms to enable the successful development of an appropriate solution.

To continue, agency management must commit resources to explore ways to address the need or opportunity. Management must also determine if staff or other resources will be devoted to defining and evaluating alternative ways to respond to the identified need or opportunity. At this point, the decision to proceed generally may be supported by a Feasibility Study accompanied by a Cost Benefit Analysis (CBA). A Feasibility Study in conjunction with a CBA should provide information that management needs to make decisions to initiate or continue the development, procurement and modification of proposed project (FIPS PUB 64 1.3). The process used is the same process followed under the Departments' IT Capital Investment Management selection process.

3.3.4 Perform Initial Risk Planning

A process for identifying, assessing, monitoring, reporting, and mitigating project risks is identified and documented in a Risk Management Plan. Project risks are identified and analyzed to determine any negative scope, technical, cost, and schedule risks to the project.

Frequent review points are identified when the project is divided into manageable tasks and activities. By authorizing effort to be expended only for the next phase and by requiring approval to proceed beyond that point, senior management can limit exposure to only the cost of the next phase. Further, because confidence in estimates is strongest for the next immediate phase and is less predictable for subsequent phases, management may assume they are authorizing work to be performed against an estimate that is reasonably reliable. To facilitate risk management at the end of each phase, the SDLCM methodology requires a detailed and accurate time and cost projection for the next phase, while permitting a less detailed time and cost estimate for the balance of the project. This enables management to make decisions in an environment where risks can be managed and controlled.

3.3.5 Establish Project Manager, System Owner, and User Representatives

After core deliverables are reviewed and accepted Agency and/or executive management, the IT system project begins. Identify essential project personnel. Designate a Project Manager having the appropriate skills, experience, credibility, and availability to lead the effort. Identify the System

Owner point of contact and support personnel from key organizations.

3.3.6 Determine Security Classifications

A determination is made whether the IT development, modification, or enhancement requires a security classification (See DOL Computer Security Handbook). Sensitive systems must be identified (as per Public Law 100-235, The Computer Security Act of 1987). Coordination between the CIO and appropriate Agency officials takes place to ensure posting in the Federal Register.

3.4 Phase Deliverables

Deliverables produced and/or updated in the Conceptual Planning Phase are described below. Deliverables are reviewed and approved by the designated reviewing authority before moving to the next phase.

3.4.1 Core Deliverables

Core deliverables are those that are required during this phase. If the project is a new IT development effort, the core deliverables are initiated during this phase and subsequently updated in later phases, as appropriate. If the project represents a modification or enhancement to an existing system, then the existing core documents are updated as appropriate. The following core deliverables are initiated, or updated if they already exist, during the Conceptual Planning Phase:

- RITS/Statement of Concept - An agreement between the requesting organization and the IT organization reviewing the request is reached. Decisions are made as to when the project will be initiated, the target completion date and resources needed from both the user community and the IT organization to ensure a successful implementation.

- Cost-Benefit Analysis (CBA) - The CBA provides cost and benefit information for analyzing and evaluating alternative solutions to a problem and for making decisions about initiating, as well as continuing, the development of information processing-related services. Two sample formats for producing a Cost Benefit Analysis are provided in Appendix B. See Clinger-Cohen Act 1996, IEEE 12207.0-1996 Section 5.1.1.2(c).

- Risk Management Plan - The Risk Management Plan provides an assessment of potential outcomes of a project and the likelihood that one or more unsuccessful outcomes may result. It provides a controlled mechanism to monitor, report, and direct all risk mitigation activities. It also describes how risks are accepted, transferred, or mitigated. The plan documents and identifies project risks: the analysis, assessment, and prioritization of those project risks; and plans to implement actions to reduce project risks throughout the project life cycle. A sample format for a Risk Management Plan is provided in Appendix B. See

Clinger-Cohen Act 1996 Section 5122(a)(b)(c), OMB Director's Policy Memorandum M-97-02 (Raines Rules), IEEE/EIA 12207.0-1996 Section 5.1.1.6, NIST Handbook (March 1995), OMB A-130 Appendix III B, IEEE/EIA 12207.2-1997 Section 7.1.2.1(f)/ Annex L.

- Project Management Plan (PMP) - The PMP provides a vehicle for documenting project scope, tasks, schedule, allocated resources, and interrelationships with other projects. It also provides details on the involved agency units, required job tasks, milestone and review scheduling. It is one of several key-planning documents that use a building block approach to planning. A sample format for a PMP is provided in Appendix B. See IEEE/EIA 12207.2-1997 Section 5.2.4.2.

3.4.2 Optional Deliverables

The following optional deliverables may be initiated during the Conceptual Planning Phase:

- Feasibility Study - A Feasibility Study provides an overview of a business requirement or opportunity and determines if feasible solutions exist before resources are committed. It is an Agency sponsored activity. A sample format for a Feasibility Study is provided in Appendix B. See Clinger-Cohen Act 1996 Section 5122(b) and 5123, IEEE/EIA 12207.2-1997 Section 7.1.1.1, and OMB A-130, Appendix IV, Section 8b(1).

- Acquisition Strategy - An Acquisition Strategy describes the methods to be used for acquiring necessary hardware, software, telecommunications capabilities, and contract support services. The Acquisition Strategy, if developed during this phase, evolves into an Acquisition Plan that becomes a core document in the Design Phase (see Chapter 5). See OMB Director's Policy Memo –97-02 (Raines rules), Clinger-Cohen Act 1996 Section 5124, OMB A-130 Appendix IV Section 8b(5), OMB A-109, IEEE/EIA 12207.0-1996 Sections 5.1.1.8, and 5.2.4.

- Work Breakdown Structure (WBS) - The WBS defines the product to be developed and relates the elements of work involved to each other and to the end product. The WBS, if developed during this phase, is updated in subsequent Planning and Requirements Definition Phase and becomes a core deliverable in the Design Phase (see Chapter 5). See IEEE/EIA 12207.2-1997 Section 5.2.4.5 (c).

- Statement of Work (SOW) - A SOW presents the scope of the work that is to be investigated and the objectives to be accomplished. See Clinger-Cohen Act 1996 Section 5312.

3.5 Phase Considerations

Key considerations during this phase may address the following questions:

- Is it feasible to proceed (i.e., is the IT need or opportunity beyond the capabilities of existing systems and is developing a new system a promising approach)?
- Are the projected benefits of the proposed IT system effort justify the project costs and resources needed?
- Are appropriate funding and other needed resources available to proceed?
- Have project risks been examined and reviewed by all parties concerned and a risk management plan appropriately documented?
- Has a security classification been established?
- Has a User Group been established (if needed, at the discretion of the Agency)?

Systems Development and Life Cycle Management (SDLCM)

4. PLANNING AND REQUIREMENTS DEFINITION PHASE

4.1 Phase Overview

The Planning and Requirements Definition Phase begins after the project has been defined and appropriate resources have been committed. There are two essential aspects of this phase: 1) planning, and 2) defining the functional requirements that the system will need to address. It is during this phase that the Project Management Plan is updated to include or provide additional detail regarding the development approach and methods, tools, tasks, resources, and schedules. Functional requirements are defined to address data, system performance, security, and maintainability aspects of the system. Exhibit 4-1 identifies key inputs, activities, and deliverables of this phase.

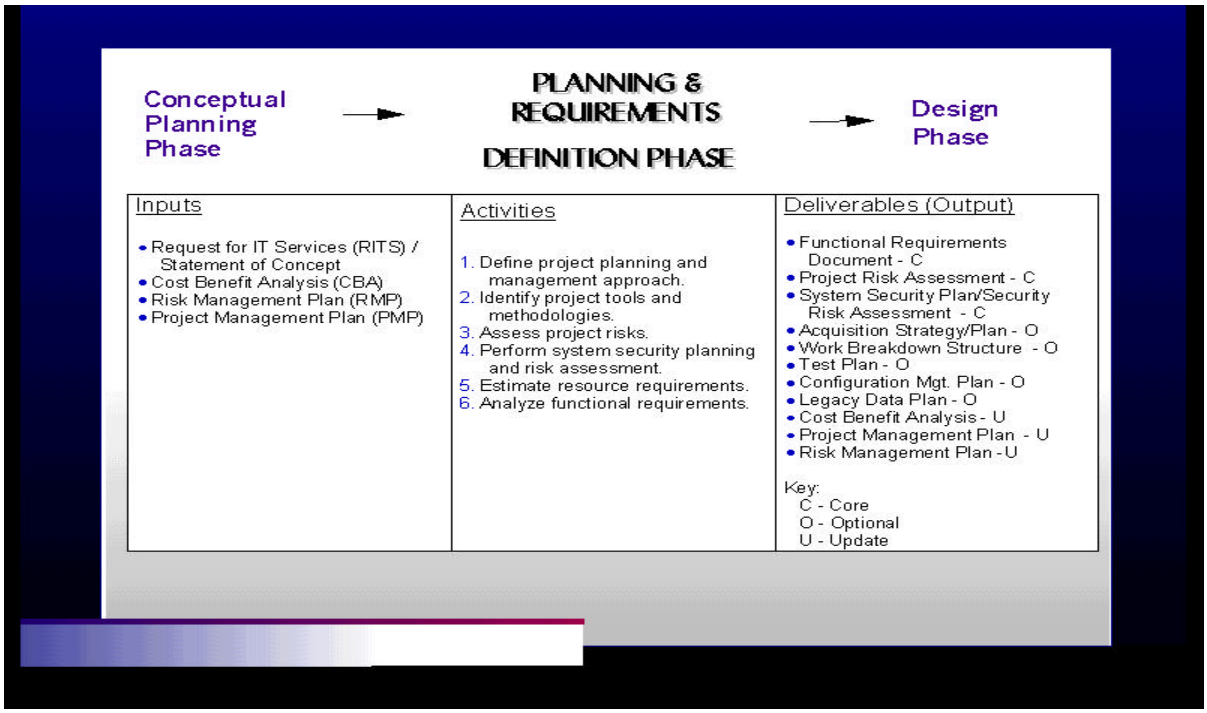


Exhibit 4-1: Planning and Requirements Definition Phase Inputs, Activities, Deliverables

4.2 Phase Inputs

The key inputs to the Planning and Requirements Definition Phase are the core deliverables that were produced during the Conceptual Planning Phase. They are:

- Request for Information Technology Services (RITS)/Concept Statement
- Cost Benefit Analysis (CBA)
- Risk Management Plan (RMP)
- Project Management Plan (PMP)

Depending on the strategy adopted, a SOW may or may not be an input to this phase. Normally, the business need for a solution is described in a SOW, based on the strategic planning process, a legislative mandate, a user problem report, or a user proposal.

4.3 Phase Activities

4.3.1 Define Project Planning and Management Approach

The methodology to be adopted for the IT effort, based on the SDLCM work pattern selected (see Chapter 2, SDLCM Work Patterns), is defined and customized. For large or complex systems, it may be appropriate to divide the system into major subsystems and manage the evolution of each subsystem through the life cycle. However, for such systems, proper coordination across the subsystems is necessary to ensure consistency and successful integration. How phase activities are to be documented, reviewed, and approved are identified and planned. Other factors related to defining the project planning and management approach include the following:

- Identifying the SDLCM work pattern and any tailoring aspects. This information should be included in the IT system Project Management Plan.

- Establishing project schedules. This information should be documented in the IT system's Project Management Plan and should allocate time for routine systems maintenance activities such as: conversion/upgrades of hardware and software; removal of defects or minor modifications to reflect changes in the business or technical environment or legislation; alteration, rewriting, or restructuring of a system to reduce the maintenance effort or to make operations more efficient.

- Planning for emergency maintenance and establishing procedures to address sudden breakdowns due to hardware or software failure.

- Managing life cycle activities by setting specific milestones for measuring the work

completed to the costs incurred during the life cycle. See Clinger-Cohen Act 1996 Section 5122 (b) (1) and (3).

4.3.2 Identify Project Tools and Methodologies

The organization of the project, the specific SDLCM work pattern to be adopted, and methodologies and tools to be used in this phase and subsequent phases are identified and planned for in this phase. The set of methods and tools may include prototyping and utilization of computer-aided software engineering tools, as well as the needs for linking the tools across all subsequent life cycle phases and activities.

4.3.3 Assess Project Risks

Assessing an IT system's project risk entails analyzing its information needs and vulnerabilities. Recommended actions necessary to reduce identified risks are determined. Project risks are identified, analyzed, assessed and categorized by severity with the highest risk at the top and the lowest risk at the bottom. The results of the assessment are documented in a Project Risk Assessment (or may be part of the overall Risk Management Plan) and includes a list of vulnerabilities and recommended measures to overcome/lessen such risks. Assessing project risks is an ongoing activity where previously identified risks are reassessed during subsequent phases and new risks identified. Project risk assessments produce information that can help a Project Manager, and site senior manager make decisions on even operating at an acceptable level of risk. Conducting a Project Risk Assessment for a system is typically at the following times:

- Before development and operational use of a new system.
- When there is a significant modification to the operational environment or configuration baseline of an existing system specifically concerning interfaces.
- At periodic intervals or at least once a year, commensurate with the risk assessment of the information processed by a system.

The Project Manager is responsible for coordination with the Chief Security Officer (CSO) or designee for implementing a security project risk assessment.

4.3.4 Perform System Security Planning and Security Risk Assessment

All Federal IT systems have some level of sensitivity and require protection from being accessed by unauthorized sources. As such, it is imperative, that System Security Plans (SSP)/Security Risk Assessments (SRA) be developed to safeguard against any intrusions. The problem becomes even more acute if systems have multiple interfaces to other similar sensitive systems. SSP/SRAs are living dynamic documents that are initiated in this phase and are updated through the life cycle process. SSP/SRAs need to be updated every 3 years or when there is a significant change or

modification to the system. Other activities that are done as part of the SSP/SRA are defined in the DOL Computer Security Handbook as part of the SSP/SRA and include:

- All SSP/SRA systems need to be identified by unique DOL Identification Numbers.
- Personnel working on such systems need to be cleared to the appropriate level of the security classification of the system. This applies both to employees and contractor personnel.
- Ongoing regular training on the different aspects of security needs to be planned.
- Each page of the SSP/SRA should be marked on the bottom, front of each page as Sensitive Information in bold font.
- Audit trails of transactions and documentation need to be established.
- Systems that are interconnected for sharing sensitive data/information need to have signed and approved Memorandums Of Understanding (MOU)/Agreements in place before establishing the interconnection. See OMB Circular A-130.
- A network diagram or schematic to help identify, define and clarify the system boundaries for the system and the interconnections to other networks (LAN/WAN) should be prepared and maintained.

4.3.5 Estimate Resource Requirements

Estimating human resource requirements for staffing a project is a key activity of project planning and should be done in conjunction with evaluating the scope of the project, identifying the tasks and deliverables, estimating the required resource hours, distributing resource hours and leveling resources and reviewing the preliminary estimates thoroughly. Another essential activity of project resource planning is estimating hardware and software requirements and available resources to determine the availability and suitability for project applications.

4.3.6 Analyze Functional Requirements

Requirements analysis and definition during this phase involves an iterative analysis of system-level requirements that are then defined in terms of high-level functional and data requirements. Documentation related to user requirements from the previous phase is used as the basis for further analysis and for the development of functional requirements. The analysis may reveal new insights into the overall information systems requirements and the related deliverables should be revised accordingly. The system is defined in terms of functions to be performed. The requirements are defined to a level of detail sufficient for system design to proceed. During the Design Phase, these high-level functional requirements are further analyzed and defined in terms of detailed functional and data requirements that address data, system inputs, processes, outputs, interfaces (both internal and external), security, and maintainability aspects of the system.

Functional requirements are documented in a Functional Requirements Document (FRD). This document addresses the activities that need to be performed to analyze, understand, and review the overall architecture of the proposed system, the extent of interfaces with other existing

internal/external systems or systems currently under development. In addition, activities may also relate to the high-level data and functional requirements, user organization definition, and the ability of existing system or data resources to satisfy system requirements.

In addition to analyzing functional requirements from a system's perspective, planners must be cognizant of additional considerations that must be addressed during the Planning and Requirements Definition Phase. Several references cited below are exemplars demonstrating that laws, regulations and policies may apply.

The Americans with Disabilities Act and Section 508 of the Rehabilitation Act require, regardless of the system development effort, that electronic and information technology allow individuals with disabilities to have appropriate access and use of information and data that is comparable to access and use of information and data by people who do not have a disability (P. L. 105-220). For additional information, see the Federal IT Accessibility Initiative at www.section508.gov.

Planners are also responsible for ensuring the privacy, confidentiality, integrity, and availability of citizen and employee information. The DOL recognizes that privacy protection is both a personal and fundamental right of all citizens and employees. Among the most basic of citizens' and employees' rights is an expectation that the DOL will protect the confidentiality of personal, financial, and employment information. Citizens and employees also have the right to expect that DOL will collect, maintain, use, and disseminate identifiable personal information and data only as authorized by law and as necessary to carry out mission responsibilities. Citizen and employee information is protected by the following:

- Privacy Act of 1974, as Amended (5 USC 552a) which affords individuals the right to privacy in records that are maintained and used by Federal agencies. Note that 5 USC 552a includes the Computer Matching and Privacy Act of 1988 (Public Law 100-503);

- Computer Security Act of 1987 (Public Law 100-235) which establishes minimum security practices for Federal computer systems;

- OMB Circular A-130, Management of Federal Information Resources, which provides instructions to Federal agencies on how to comply with the fair information practices and security requirements for operating automated information systems;

- Freedom of Information Act, as Amended (5 USC 552) which provides for the disclosure of information maintained by Federal agencies to the public while allowing limited protections for privacy.

4.4 Phase Deliverables

Deliverables produced and/or updated in the Planning and Requirements Definition Phase are described below. Deliverables are reviewed and approved by the designated reviewing authority before the IT system moving to the next phase.

4.4.1 Core Deliverables

Core deliverables are those that are required during this phase. If the project is a new IT development effort, the core deliverables are initiated during this phase and subsequently updated in later phases. If the project represents a modification or enhancement to an existing system, then the existing core documents are updated as appropriate. The following core deliverables are initiated, or updated if they already exist, during the Planning and Requirements Definition Phase:

- Functional Requirements Document (FRD) — The FRD is a formal statement of an application's business requirements, and serves the same purpose as a contract. The developers agree to provide the capability specified and the client agrees to find the product satisfactory if it provides the specified capabilities. A sample outline for an FRD is provided in Appendix C. See IEEE/EIA 12207.0-1996 Sections 5.1.1.2//5.2.4.3.

- Project Risk Assessment (PRA) — A PRA examines risks to the system and examines the potential impacts on the mission due to loss or degradation of automated information system resources. It may describe how risks are accepted and transferred. The PRA may be part of the Risk Management Plan. See Clinger-Cohen Act 1996 Section 5122(a)(b)(5), OMB Director's Policy Memo M-97-02 (Raines Rules), IEEE/EIA 12207.0-1996 Section 5.1.1.6, OMB A-130 Appendix III B, IEEE/EIA 12207.2-1997 Section 7.1.2.1(f)/ Annex L.

- System Security Plan (SSP)/Security Risk Assessment (SRA) – All Federal IT systems have some level of sensitivity and require protection as part of good management practice. One aspect of managing an IT system is the development of a SSP/SRA that documents the protection afforded to the system by technical, managerial, and operational means. Furthermore, the implementation of a SSP/SRA is required by OMB A-130 and the Computer Security Act 1987 (CSA). An SSP/SRA is a living, dynamic document reflecting the current posture of the IT system and should be initially developed in the Planning and Requirements Definition Phase and updated in later phases. It should be updated after a significant system configuration change, or at least once in every 3 years. See OMB A-130 Section 8 and Appendix III Ba2, IEEE/EIA 12207.0-1996 Section 5.2.4.5, Clinger-Cohen Act 1996 Section 5131, and DOL Computer Security Handbook.

4.4.2 Optional Deliverables

The following optional deliverables may be initiated during the Planning and Requirements Definition:

- Acquisition Strategy - An Acquisition Strategy describes the methodology to be followed for

acquisition of resources required for project execution. The Acquisition Strategy, if developed during this phase (or updated if initially developed during the Conceptual Planning Phase, evolves into an Acquisition Plan during the Design Phase (see Chapter 5). See OMB Director's Policy Memo –97-02 (Raines Rules), Clinger-Cohen Act 1996 Section 5124, OMB A-130 Appendix IV Section 8b(5), OMB A-109, IEEE/EIA 12207.0-1996 Sections 5.1.1.2, and 5.2.4.

- Work Breakdown Structure (WBS) - WBS defines the product to be developed and relates the elements of work to be accomplished to each other and to the end product(s). It is often produced as part of the PMP. The WBS, if developed during this phase, becomes a core deliverable in the Design Phase (see Chapter 5). Additional information is provided in Appendix B (see PMP). See IEEE/EIA12207.2-1997 Section 5.2.4.5 (c).

- Configuration Management (CM) Plan - The CM Plan establishes uniform CM practices in a system development project to manage the establishment of, and changes to, system hardware and software. The CM Plan, if developed during this phase, becomes a core deliverable in the Design Phase (see Chapter 5). A sample format for a CM Plan is provided in Appendix D. See IEEE/EIA 12207.2-1997 Section 6.2, IEEE/EIA 12207.0-1996 Section 5.2.4.5, and ISO 10007.

- Test Plan - Based on the functional requirements document, a preliminary Test Plan may be initiated in this phase. The Test Plan establishes a minimum acceptable performance level and conformance to the stated requirements. The plan is refined during the later phases to ensure that all aspects of the system are adequately tested and can be implemented. Test Plans become core deliverables in the Development and Test Phase (see Chapter 6). A sample format for a Test Plan is provided in Appendix E. See IEEE/EIA 12207.2-1997 Annex D H.4(c).

- Legacy Data Plan - Sometimes the upgrading of a system or parts of a system will create legacy data, i.e., and old data in a format that cannot be processed by the new system. The Legacy Data Plan identifies the time period covered by the data, volume of data, and where it resides. If some or all legacy data have already been converted to a new format, the approach to testing the converted data must be discussed. Requirements for processing legacy data in the future and plans for meeting those requirements are provided. It is acceptable to say that data will be converted if they are needed in the future, but information about what is required for the conversion process must be provided. This information includes a discussion of resource requirements for doing the conversion and potential problems that would need to be overcome. See IEEE/EIA 12207.2-1997 Section 5.5.5.

4.4.3 Updated Deliverables

The following documents generated during the Conceptual Planning phase may be updated during this phase. These are living documents that evolve throughout the life cycle and are updated, as

needed, to reflect the current level of maturity of the project.

- Project Management Plan (PMP) – The PMP is updated to include updated resources allocation and scheduling information. Additional project planning activities are documented or updated including the development approach, methods, tools, tasks, resources, schedules, and user inputs. The plan is prepared based on the information available and will be updated and refined in the subsequent phases. Consideration of disabled personnel is made in accordance with the Physical Disabilities Act of 1990. A sample format for a PMP is provided in Appendix B. See IEEE/EIA 12207.2-1997 Section 5.2.4.2.

- Cost Benefit Analysis (CBA) – The CBA is updated to include additional tangible/intangible benefits that may accrue along with variations in the budgeted costs. Two sample formats for producing a Cost Benefit Analysis are provided in Appendix B. See Clinger-Cohen Act 1996 sec. 51122(c), IEEE 12207.0-1996 Section 5.1.1.6

- Risk Management Plan (RMP) – The RMP is updated to include improved risk management/reduction efforts, using customized tools and similar devices. A sample format for a Risk Management Plan is provided in Appendix B. See Clinger-Cohen Act 1996 Section 5122(a)(b)(5), OMB Director's Policy Memorandum M-97-02 (Raines Rules), IEEE/EIA 12207.0-1996 Section 5.1.1.6, NIST Handbook (March 1995), OMB A-130 Appendix III B, IEEE/EIA 12207.2-1997 Section 7.1.2.1(f)/ Annex L.

4.5 Phase Considerations

Automated project scheduling systems facilitate the production of initial project staffing estimates and permit a regular review of staffing projections throughout the life cycle. Actual-to-estimated comparisons should be made and maintained, and forwarded to estimators to help improve estimating skills. Subsequent work includes refining the requirements, defining the solution, and confirming the project management approach. The end of this phase is a critical juncture for the project; it is the point at which agreements between the Project Manager and System Owner are made, to procure the resources required for accomplishment of the remaining phases of the project life cycle. This can be addressed by answering the following question:

- What resources are needed for completion of the remaining phases of the Life Cycle?

Systems Development and Life Cycle Management (SDLCM)

5. DESIGN PHASE

5.1 Phase Overview

Upon completion of the Planning and Requirements Definition Phase, the system progresses to the Design Phase. During this phase, functional requirements are translated into preliminary and detailed designs. Decisions are made to address how the system will meet functional, physical, interface, and data requirements. A preliminary (general) system design emphasizing the functional features of the system is produced as a high level guide. Then a final (detailed) system design is produced which expands the design by specifying all the technical detail needed to develop the system. Exhibit 5-1 identifies key inputs, activities, and deliverables of this phase.

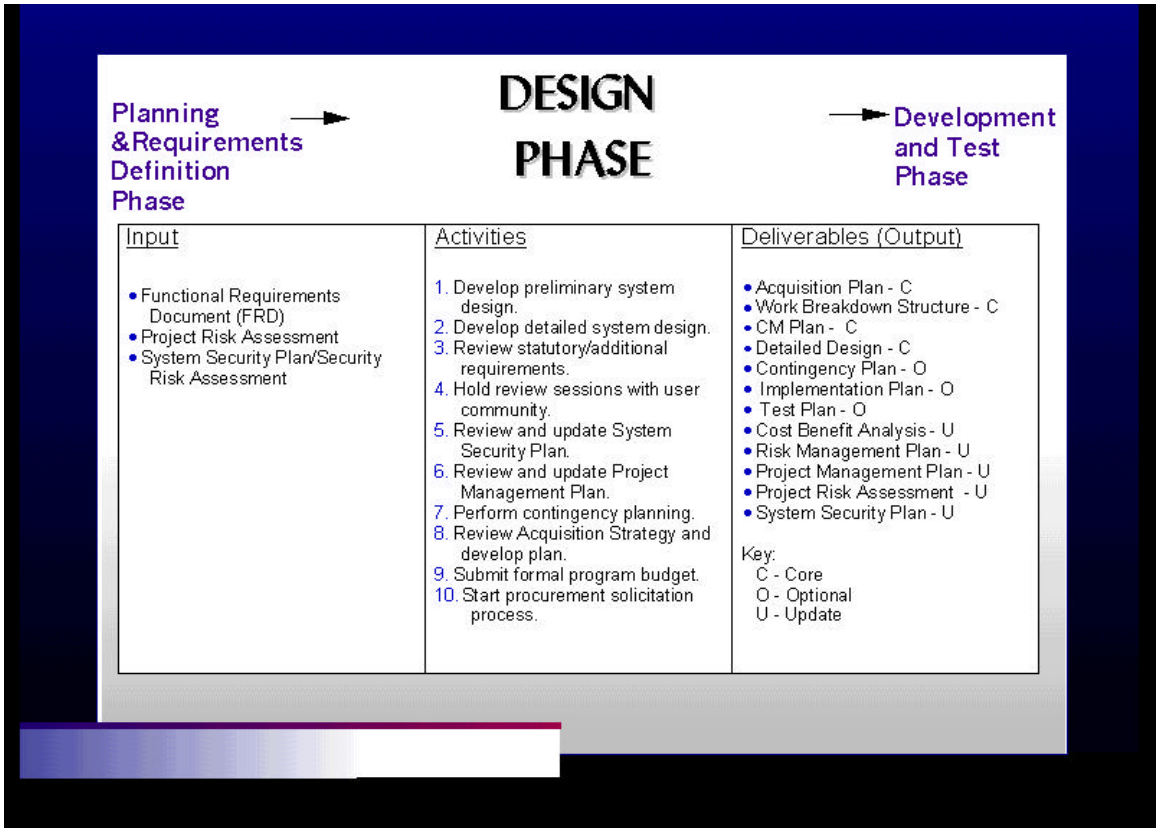


Exhibit 5-1: Design Phase Inputs, Activities, Deliverables

5.2 Phase Inputs

The key inputs to the Design Phase are the core deliverables that were produced during the Planning and Requirements Definition Phase. They are:

- Functional Requirements Document (FRD)
- Project Risk Assessment
- System Security Plan/Security Risk Assessment

5.3 Phase Activities

5.3.1 Develop Preliminary System Design

The preliminary system design clarifies the general characteristics of the system. It specifies the operating system, architecture components, their timing and sizing, external and internal interfaces, inputs and outputs of each subsystem, administrative activities, and security and auditing needs. It serves the same purpose as the initial design of a building and is the foundation for further detailed design. See IEEE/EIA 12207.2-1997 Section 5.3.4.2/ 5.3.5.6/ 5.3.7.5/ 5.3.8.5 and NIST Special Publication 500-223 Section 2.2/ 2.3.

5.3.2 Develop Detailed System Design

The preliminary design is the foundation for the detailed design. System components are further specified into modules, processes, data, and interfaces and are defined to a level of detail that will enable a smooth transition to the Development and Test Phase. This top-down approach follows the structure previously set and adds substructure so that developers need minimal additional guidance. The detailed design is documented in the Detailed Design Document, a core deliverable of this phase.

5.3.3 Review Statutory/Additional Requirements

After the design review is completed, statutory or additional requirements may be identified that necessitate a revision to prior phase decisions or documents. Alternatively, these may lead to a new project.

5.3.4 Hold Review Sessions with User Community

As the design is initiated, participation from the user community is essential to ensure that the requirements and the design will be consistent with the new or enhanced business requirements.

5.3.5 Review and Update System Security Plan

The application/system developer should identify specific security requirements, allocate them to specific modules in the design, and update the System Security Plan, as needed to reflect any changes. For example, if a requirement exists to audit a specific set of user actions, the developer may have to add a workflow module into the design to accomplish the auditing.

Public Law 100-23 5, the Computer Security Act of 1987, requires Federal agencies to prepare security plans for systems that process, store, or transmit sensitive information. A security plan is the primary reference point that documents the nature and extent of all security-protective measures designed to safeguard the facility, equipment, personnel, and information processed or stored by automated data processing operating within the facility. The plan focuses on specific protective measures and any special policies or procedures set up for a system. See the DOL Computer Security Handbook for pertinent or related material.

5.3.6 Review and Update Project Management Plan

As tasks are completed in this phase, the project manager will update the Project Management Plan as needed. Project planning information, such as schedules, resources, and project tools and methodologies are updated to reflect changes in approaches and decisions.

5.3.7 Perform Contingency Planning

Contingency planning is optional in the Design Phase. The objective is to ensure that DOL systems are able to recover from processing disruptions in case of localized emergencies or large-scale disasters. An emergency response plan, developed in conjunction with the System Owner and maintained at the primary and backup computer installations, ensures that reasonable continuity of support is provided if events occur that prohibit normal operations. Contingency Plans must be routinely reviewed, updated, and tested to enable vital operations and resources to be restored as quickly as possible and to keep system downtime to an absolute minimum.

5.3.8 Review Acquisition Strategy and Develop Plan

The acquisition strategy, if developed during the Conceptual Planning Phase or Project Planning and Requirements Definition Phase, is reviewed for accuracy and completeness and is formalized into an Acquisition Plan. Additional detail is added, if not already specified, indicating how specific equipment or resources are to be acquired.

5.3.9 Submit Formal Program Budget

Initiation of a budget request is performed at this stage to alert all affected parties of the costs that will incur if the project should continue through the implementation phase. Proper approvals are necessary to obtain the required funding in order to proceed.

5.3.10 Start Procurement Solicitation Process

Upon completion of the formal budget process, purchase orders for all required hardware, software, and telecommunications equipment are submitted to the Agency's procurement organization.

5.4 Phase Deliverables

Deliverables produced and/or updated in the Design Phase are described below. Deliverables are reviewed and approved by the designated reviewing authority before the IT system moving to the next phase.

5.4.1 Core Deliverables

Core deliverables are those that are required during this phase. If the project is a new IT development effort, the core deliverables are initiated during this phase and subsequently updated in later phases. If the project represents a modification or enhancement to an existing system, then the existing core documents are updated as appropriate. The following core documents are initiated, or updated if they already exist, during the Design Phase.

- Detailed Design – The Detailed Design is an extension of the preliminary design activity. It involves filling in the details implied by the preliminary design. Subsystems may be further subdivided and described using charts and pseudo code. Logic specifications are given and data usage is defined in detail. User input and user approvals are spelled out. It also includes detailed system requirements used to develop the system. Changes to the detailed design due to changes in the preliminary design may create additional costs and delays that may require revisions to the schedules set in the Project Management Plan. A sample outline for a Detailed Design Document is provided in Appendix D. See IEEE/EIA 12207.2-1997 Section 5.3.4.2/ 5.3.5.6/ 5.3.7.5/ 5.3.8.5 and NIST Special Publication 500-223 Section 2.2/ 2.3.

- Work Breakdown Structure (WBS) - The WBS defines the product to be developed and relates the elements of the work involved to each other and to the end product. It describes these arrangements in a manner that promotes verification and measurement of technical accomplishments, and it provides a conceptual framework for integrated planning and control. The WBS supplements the Project Management Plan. It is optional in the first phase, Conceptual Planning, and optional in the second phase, Planning and Requirements Definition, but it is a core deliverable for Design. In the Development and Test Phase, the WBS is updated. The WBS should be distinguished from the Contract WBS. Additional detail is provided in Appendix B**.** See IEEE/EIA12207.2-1997 Section 5.2.4.5 (c).

- Configuration Management (CM) Plan - Systematic control of revisions is necessary to enable reproduction of past results from a team effort. This plan identifies the automated

CM system to be used for software development, and other items to be placed under control, with methods of control. Locations where items are stored are specified and plans for audits are specified. This document is optional in the prior Planning and Requirements Definition Phase, becomes a core deliverable in this phase, and is updated in the Development and Test Phase. Starting in the prior phase may optimize the workload in this phase. A sample outline for a CM Plan is provided in Appendix D**.** See IEEE/EIA 12207.2-1997 Section 6.2 and ISO 10007.

- Acquisition Plan - The Acquisition Plan follows from the Acquisition Strategy, if developed and/or updated in the previous two phases. It describes the methods to be used in acquiring necessary hardware, software, telecommunication capabilities, and contractor support services. It promotes planning and verification that necessary resources will be available when needed. A milestone schedule emphasizes this. During this phase, as the details of the system are defined, resources that need to be acquired are identified. A sample outline for an Acquisition Plan is provided in Appendix D. See OMB Director's Policy Memorandum M- 97-02 (Raines Rules), Clinger-Cohen Act 1996 Section 5124, OMB A-130 Appendix IV Section 8b(5), OMB A-109, IEEE/EIA 12207.0-1996 Sections 5.1.1.2, 5.1.1.8, and 5.2.4.

5.4.2 Optional Deliverables

The following optional deliverables may be initiated during the Design Phase:

- Contingency Plan - The Contingency Plan documents the sequence of events and actions that will enable DOL to continue to function if the new system does not meet business requirements. See OMB A-130 Appendix III A3 b(2)d.

- Implementation Plan – The Implementation Plan describes how the system is to be implemented and includes: a description of the implementation activities; an implementation schedule; support needed for implementation; personnel and roles and responsibilities; training; performance monitoring; site unique requirements; and verification methods. It includes back-off plans for use when necessary. It is optional during the Design Phase, but it becomes a core deliverable during the subsequent Development and Test Phase as the implementation details are further defined. Training, project planning, and testing components of the Implementation Plan must be consistent with the Training Plan, PMP, and Test Plan. A sample outline for an Implementation Plan is provided in Appendix E**.** See IEEE/EIA 12207.2-1997 Section 5.3.1.

- Test Plan – The Test Plan documents the test environment, resources, training, methods, sequence, evaluation, and test descriptions. For larger systems it should be begun early to minimize oversights. Although optional at this phase, early test definition can begin to include the definition of test approach, test scenarios, identification of test tools, simulators, and special test requirements. Test schedules and approach components of the Test Plan

must be consistent with the Implementation Plan and PMP. The Test Plan becomes a core deliverable in the Development and Test Phase (see Chapter 6). A sample outline for a Test Plan is provided in Appendix E. See IEEE/EIA 12207.2-1997 Annex D-H.4(c).

5.4.3 Updated Deliverables

The following documents generated during the Conceptual Planning Phase and Planning and Requirements Definition Phase may be updated during this phase. These are living documents that evolve throughout the life cycle and are updated, as needed, to a level of detail that reflects the maturity of the project.

- Project Management Plan (PMP) - The PMP is a core deliverable of Conceptual Planning and is subsequently updated during this phase to reflect design decisions. Project planning information, such as schedules, resources, and project tools and methodologies, are updated to reflect changes in approaches and decisions. The PMP is updated to reflect implementation and testing plans reflected in the Implementation Plan and Test Plan, respectively. A sample outline for a PMP is provided in Appendix B. See IEEE/EIA 12207.2-1997 Section 5.2.4.2.

- Risk Management Plan (RMP) - The RMP is a core deliverable of Conceptual Planning, and is subsequently updated through five life cycle phases, including the Operations and Maintenance Phase. As the project advances, previously identified risks are re-evaluated and newly realized risks are defined and assessed. A sample outline for an RMP is provided in Appendix B. See Clinger-Cohen Act 1996 Section 5122(a)(b)(5), OMB Director's Policy Memorandum M-97-02 (Raines Rules), IEEE/EIA 12207.0-1996 Section 5.1.1.6, NIST Handbook (March 1995), OMB A-130 Appendix III B, IEEE/EIA 12207.2-1997 Section 7.1.2.1(f)/ Annex L.

- Project Risk Assessment – The Project Risk Assessment is updated during this phase to address the re-evaluation of previously identified risks as well as additional risks that may have been identified during design activities. This assessment may be a part of the RMP. See OMB A-130 Section 8 and Appendix III Ba2, IEEE/EIA 12207.0-1996 Section 5.2.4.5, and Clinger-Cohen Act 1996 Section 5131.

- System Security Plan (SSP)/Security Risk Assessment (SRA) – The SSP/SRA is a living, dynamic document reflecting the current posture of the IT system and should be initially developed in the Planning and Requirements Definition Phase and updated in later phases. More specificity is added in this phase to reflect design decisions. It is also updated after a significant system configuration change, or at least once in every 3 years. See OMB A-130 Section 8 and Appendix III Ba2, IEEE/EIA 12207.0-1996 Section 5.2.4.5, Clinger-Cohen Act 1996 Section 5131, and DOL Computer Security Handbook.

- Cost-Benefit Analysis (CBA) – The CBA is updated in this phase as needed to include

additional tangible or intangible benefits that may accrue along with the budgeted costs. A sample format for a CBA is provided in Appendix B. See Clinger-Cohen Act 1996, IEEE 12207.0-1996 Section 5.1.1.6.

5.5 Phase Considerations

Key considerations during this phase may address the following questions:

- Has a sufficient dialog occurred with the designated future users to document their needs before writing the preliminary design?
- Have all project stakeholders (Project Manager, customer, performing organization, and owner) reviewed the final design to ensure incorporation of all requirements and design considerations (see A Guide to the Project Body of Knowledge, William R Duncan, Director of Standards, Section 2.2)?
- Has proper funding been allocated to continue the implementation of the project?
- Have all significant risks been identified and documented?
- Was a Configuration Management Plan that will track, modify, and update software development entities?
- Have new management, risk, and security considerations been documented in light of new understandings flowing from the growth of the project?
- Were statutory requirements (e.g., accessibility) met?

Systems Development and Life Cycle Management (SDLCM)

6. DEVELOPMENT AND TEST PHASE

6.1 Phase Overview

During the Development and Test Phase, executable software is developed from detailed design specifications. The system is validated through a sequence of unit, integration, system, and acceptance test activities. The objective is to ensure the system functions as expected and user requirements are satisfied. Large systems are solicited, awarded, and managed in accordance with the Acquisition Plan. All hardware, system software, communications, applications, procedures, and associated documentation are developed/acquired, tested, and integrated. This phase requires strong user participation in order to verify that all requirements have been thoroughly tested and meet all business needs. Exhibit 6-1 identifies essential inputs, activities, and deliverables of this phase.

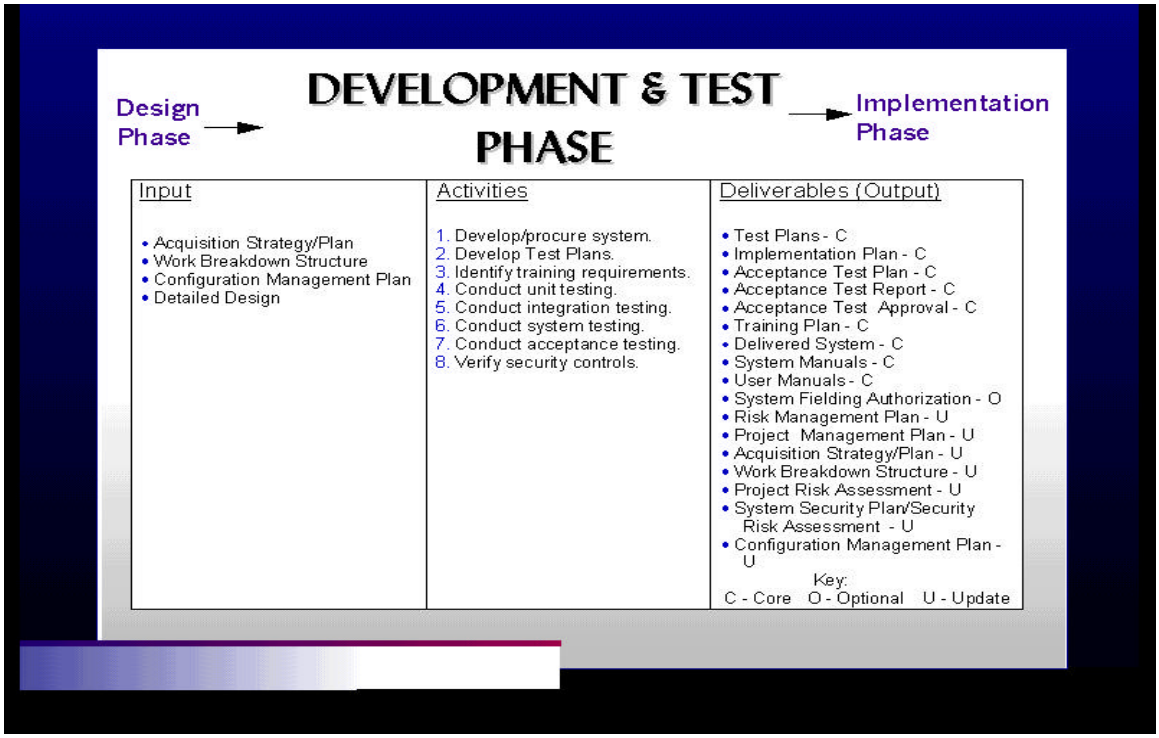


Exhibit 6-1: Development and Test Phase Inputs, Activities, Deliverables

6.2 Phase Inputs

The key inputs to the Development and Test Phase are the core deliverables produced during the Design Phase. They are:

- Detailed Design Document - contains the subsystem logic specifications and their inputs and outputs.

- Work Breakdown Structure (WBS) - The WBS defines the product to be developed and relates the elements of the work involved to each other and to the end product.

- Configuration Management (CM) Plan – Identifies the management, tracking, and control methods for maintaining system configuration items (software, hardware, documentation, change requests, etc.). It may identify an automated CM system to be used for software and other items to be placed under control.

- Acquisition Plan - describes the methods to be used in acquiring necessary hardware, software, telecommunication capabilities, and contractor support services.

6.3 Phase Activities

6.3.1 Develop/Procure System

Obtain hardware, software and other required resources. Develop the system. Identifying personnel assigned to the project, generate code, compile and link it, perform unit testing in accordance to development approach and standards defined in the Project Management Plan. Methods specified in the Configuration Management Plan are utilized to ensure system versions and changes are managed, tracked. Items to be procured include those for both development and production environment. They are procured, as needed in accordance to the process defined in the Acquisition Plan.

6.3.2 Develop Test Plans

Testing activities are planned and documented and may include test cases, test scripts, and test scenarios. Test Plans are documented at varying levels, as appropriate, to validate the detailed requirements defined in the Design Phase and functional requirements defined in the Planning and Requirements Definition Phase. Test Plans are the basis for performing integration, system, and acceptance testing activities that occur later in this phase. Test Plans must be kept consistent with the methods and schedules specified the Project Management Plan and Implementation Plan.

6.3.3 Identify Training Requirements

Training activities are planned and documented and include a training schedule, class outline, class descriptions, training materials, resources and facility requirements, and identification of the target audience. Training materials and classes are planned and coordinated with the System Owner and user community to ensure that appropriate personnel are trained on new systems or capabilities.

6.3.4 Conduct Unit Testing

Unit testing usually occurs in conjunction with module development. Individual software modules are executed and tested in a controlled environment (e.g., test data and simulated software). The software modules are validated to ensure they yield the correct results given a range of valid and invalid inputs. Upon successful completion of unit testing, testing activities advance to the next stage - integration tests.

6.3.5 Conduct Integration Testing

Integration testing is conducted in accordance to previously documented integration test plans and procedures. The objective is to validate that integrated program components, or modules, function properly and yield expected results. In a large system, modules are typically combined into logical functional groupings called subsystems and tested at this level. Upon successful completion of integration testing, testing activities advance to the next stage - system testing.

6.3.6 Conduct System Testing

System testing is conducted in accordance to previously documented system test plans. The objective is to combine all the system components (e.g. subsystems), validate that the system functions properly and meets all technical, performance, and interface requirements. Systems are tested in realistic conditions having changing and competing priorities.

6.3.7 Conduct Acceptance Testing

Acceptance testing is conducted in accordance to the Acceptance Test Plan finalized earlier in this phase. Users participate in acceptance testing to confirm that the developed system meets all user requirements identified in the Planning Requirements and Definition Phase. Acceptance testing is conducted in a simulated "real" user environment using simulated or real target platforms and infrastructures. Acceptance test results are documented in an Acceptance Test Report. Upon completion of acceptance testing, the Acceptance Test Approval is prepared by the approving authority stating that test results have been reviewed and testing successfully completed.

6.3.8 Verify Security Controls

Security controls are tested before implementing the system implementation to uncover any design and implementation flaws that would violate security policy. Security Test and Evaluation (ST&E)

may be conducted as part of system testing. It involves verifying that a system's security mechanisms are adequate, complete, and correct, and system documentation is consistent with the actual implementation.

6.4 Phase Deliverables

Deliverables produced and/or updated in the Development and Test Phase are described below. Deliverables are reviewed and approved by the designated reviewing authority before moving to the next phase.

6.4.1 Core Deliverables

Core deliverables are those that are required during this phase. If the project is a new IT development effort, the core deliverables are initiated during this phase and subsequently updated in later phases. If the project represents a modification or enhancement to an existing system, then the existing core documents are updated as appropriate. The following core deliverables are initiated, completed, or updated if they already exist, during this phase.

- Delivered System - Is developed/procured and tested in this phase. See OMB A-130 Appendix III A; IEEE/EIA 12207.2-1997 Sec 5.3.12.

- Test Plan(s) - The plan documents the test environment, resources, training, methods, schedules, evaluation, and test descriptions for unit, integration and system test activities as appropriate. Test plan development is optional for the prior Planning and Requirements Definition Phase and for the Design Phase; however in this phase it is a core deliverable so that a testing approach needs to be established before test execution. A sample outline for a Test Plan is provided in Appendix E. See IEEE/EIA 12207.2-1997 Sec 5.3.13.1 and Annex D-H.4.

- Acceptance Test Plan - This plan documents the scope, content, methodology, sequence, management of, and responsibilities for acceptance test activities. It ensures that all aspects of the system are adequately tested against requirements. See IEEE/EIA12207.2-1997 Sec 5.3.13.1 and Annex D-H.4.

- Acceptance Test Report - Documents software testing as defined in the Acceptance Test Plan. A summary of test results documenting problems encountered during testing, are attached to this report, as appropriate. See IEEE/EIA 12207.2-1997 Section 5.3.11.2; IEEE/EIA 12207.0-1996 Annex E3, 4.

- Acceptance Test Approval – Is a checkpoint where a confirmation is reached that the IT system satisfies the intent of the project and is ready to be released for implementation. It documents that acceptance test results have been reviewed and acceptance testing successfully completed and is signed by the designated approval authority. It may be

attached to the Acceptance Test Report. See IEEE/EIA 12207.2-1997 Annex D-H.4.

- System Manuals - Includes documents providing information to describe the design, development, production, distribution, operation, maintenance, and management of the system and are produced as needed to meet specific project needs. System manuals are produced during this phase and updated as needed during the operations and maintenance phase to reflect changes or enhancements. See IEEE/EIA 12207.2-1997 Section 6.1.

- User Manuals – Document instructions, guidance, and reference information relating to user execution of the system. User manuals are produced during this phase and updated as needed during the operations and maintenance phase to reflect changes or enhancements to the system. See IEEE/EIA 12207.2-1997 Section 6.1.

- Implementation Plan - Drawing on prior documents, this plan describes a plan for implementing the system in the operational environment. It translates business needs into key activities (e.g., installation, training, verification, monitoring); specifies an implementation schedule; and identifies specific personnel, hardware, software and site requirements. It includes back-off plans for use when necessary. If a preliminary Implementation has already been produced in prior phases, it is finalized in this as the implementation details become better defined. A sample outline for an Implementation Plan is provided in Appendix E. See IEEE/EIA 12207.2-1997 Section 5.3.1.

- Training Plan - Outlines the objectives, needs, strategy, and curriculum to be addressed for training users on the new or enhanced information system. The plan presents the activities needed to support the development of training materials, coordination of training schedules, reservation of personnel and facilities, planning for training needs, and other training-related tasks. Training activities are conducted in accordance with the Training Plan to teach users how to operate the system. A sample outline for a Training Plan is provided in Appendix E. See IEEE/EIA 12207.0-1996 Section 5.2.4.5 (o), OMB A-130 Appendix III A 3 a 2) b) and Clinger-Cohen Act 1996 Section 5112(i).

6.4.2 Optional Deliverables

The following optional deliverable may be developed during the Development and Test Phase:

- System Fielding Authorization (SFA) - Used to ensure that program management, site automated data processing and/or facilities operation support staff, and the user of the proposed fielded system agree that the system meets all known requirements, that it has been developed and tested in accordance with the provisions in the Project Management Plan and other SDLCM plans. The designated approval authority signs off on the SFA. See IEEE/EIA 12207.2-1997 Section 5.3.12 and NIST Special Publication 500-223 Section 2.5.

6.4.3 Updated Deliverables

The following documents generated during previous SDLCM phases may be updated during this phase. These are living documents that evolve throughout the life cycle and are updated, as needed, to a level of detail that reflects the maturity of the project.

- Project Management Plan (PMP) – The PMP is a core deliverable of Conceptual Planning, and is subsequently updated as the project advances and management has more information and additional time to improve the previous analysis and conclusions. Updating continues through four phases, into the Implementation Phase. A sample format for a PMP is provided in Appendix B. See IEEE/EIA 12207.2-1997 Section 5.2.4.2.

- Risk Management Plan (RMP) - The RMP is updated during this phase to reflect project advances, reassessment of existing risks, and identification and assessment of new risks. A sample format for a RMP is provided in Appendix B. See Clinger-Cohen Act 1996 Section 5122(a)(b)(5), OMB Director's Policy Memorandum M-97-02 (Raines Rules), IEEE/EIA 12207.0-1996 Section 5.1.1.6, NIST Handbook (March 1995), OMB A-130 Appendix III B, IEEE/EIA 12207.2-1997 Section 7.1.2.1(f)/
  Annex L.

- Acquisition Plan - The Acquisition Plan, produced during the Design Phase (see Chapter 5), is updated as needed, to address any changes needed for acquiring necessary hardware, software, telecommunication capabilities, and contractor support services. It supplements the Project Management Plan. A sample outline for an Acquisition Plan is provided in Appendix D. See OMB Director's Policy Memorandum M- 97-02 (Raines Rules), Clinger-Cohen Act 1996 Section 5124, OMB A-130 Appendix IV Section 8b(5), OMB A-109, IEEE/EIA 12207.0-1996 Sections 5.1.1.8, and 5.2.4.

- Work Breakdown Structure (WBS) - The WBS supplements the Project Management Plan and is updated during this phase to reflect any planning and tasking changes that have been made to the PMP. Additional information for a WBS (e.g., Summary WBS, Project WBS, and Contract WBS) is provided in Appendix B. See IEEE/EIA12207.2-1997 Section 5.2.4.5 (c).

- Project Risk Assessment - The Project Risk Assessment is updated during this phase to address the re-evaluation of previously identified risks as well as additional risks that may have been identified during development and test activities. This assessment may be a part of the RMP. See OMB A-130 Appendix III Ba2, IEEE/EIA 12207.0-1996 Section 5.2.4.5, and Clinger-Cohen Act 1996 Section 5131.

- System Security Plan (SSP)/Security Risk Assessment (SRA) – The SSP/SRA is a living, dynamic document reflecting the current posture of the IT system and should be initially developed in the Planning and Requirements Definition Phase and updated in later phases.

More specificity is added in this phase to reflect development and test decisions; e.g., if any modules/interfaces that have been developed affect sensitive data that might be shared among users of the system. It is also updated after a significant system configuration change, or at least once in every 3 years. See OMB A-130 Section 8 and Appendix III Ba2, IEEE/EIA 12207.0-1996 Section 5.2.4.5, Clinger-Cohen Act 1996 Section 5131, and DOL Computer Security Handbook.

- Configuration Management (CM) Plan – The CM Plan is updated in this phase, as needed, to support identification of, or changes to: the locations where configuration items are stored (electronically or hard copy); the automated libraries used to store other documentation; the software components of the system; and configuration audits that will be performed. See IEEE/EIA 12207.2-1997 Section 6.2, IEEE/EIA 12207.0-1996 Section 5.2.4.5, and ISO 10007.

6.5 Phase Considerations

Key considerations during this phase may address the following questions:

- Has the newly developed/enhanced system undergone code, testing and/or quality reviews?
- Have the appropriate parties formally accepted the newly developed system or enhancement?
- Has proper funding been allocated to continue through the remainder of the SDLCM?
- Did the test team document any discrepancies that were existed in the original specifications?

Problems or new information identified in this phase may require changes to products developed in earlier phases. If this is the case, is an alternate approach necessary and is the project ready to proceed (e.g., go/no-go decision)?

Systems Development and Life Cycle Management (SDLCM)

7. IMPLEMENTATION PHASE

7.1 Phase Overview

During the Implementation Phase, the new or enhanced system is installed in the production environment, users are trained, data is converted (as needed), and the system is turned over to the user. This phase includes efforts required to implement the system as well as to resolve any problems identified during the implementation process. Exhibit 7-1 identifies key inputs, activities and deliverables of the Implementation Phase.

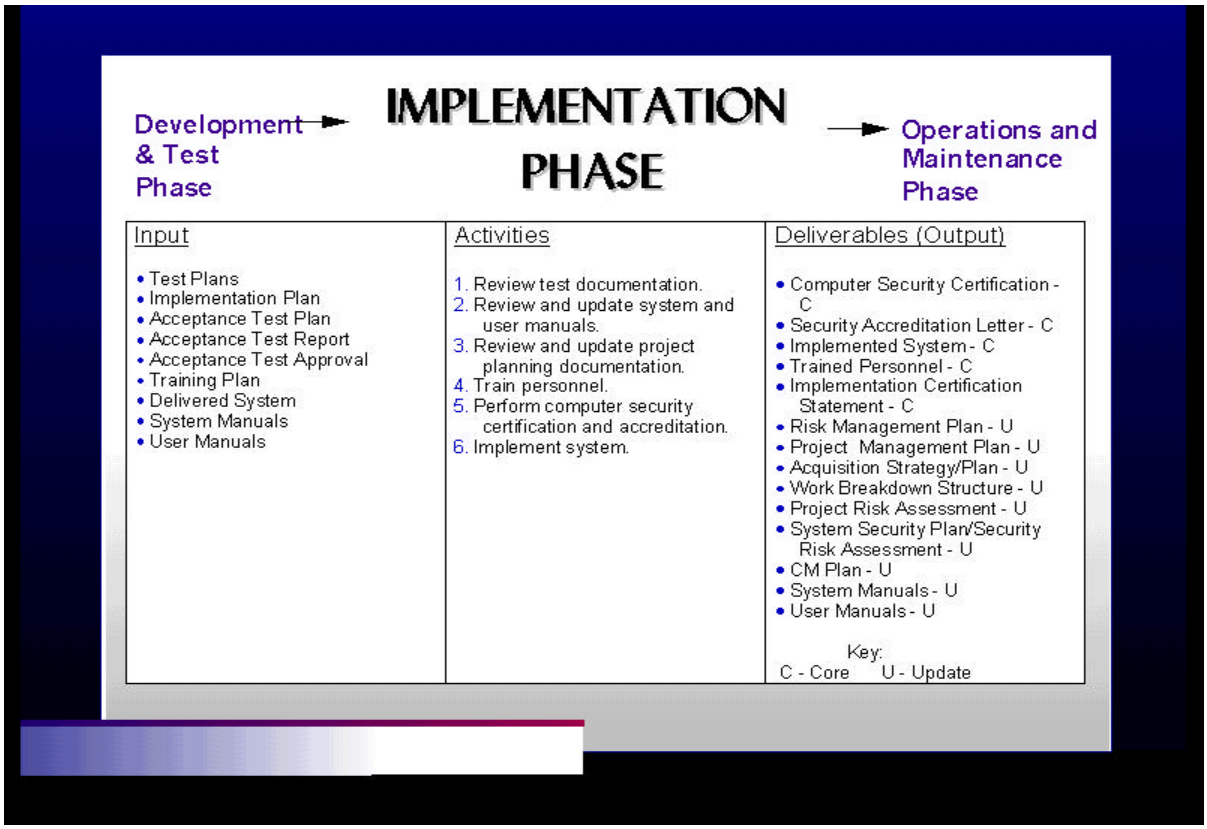


Exhibit 7-1: Implementation Phase Inputs, Activities, Deliverables

7.2 Phase Inputs

The essential inputs to the Implementation Phase are the core deliverables that were produced during the Development and Test Phase. They are:

- Test Plans
- Implementation Plan
- Acceptance Test Plan
- Acceptance Test Report
- Acceptance Test Approval
- Training Plan
- Delivered System
- System Manuals
- User Manuals

7.3 Phase Activities

7.3.1 Review Test Documentation

All test plans, test cases and test results produced during the Development and Test Phase, including those for acceptance testing, are reviewed for completeness and used within this phase. Some sample testing of the tests conducted in the previous phase may be conducted for purposes of validating system operability once the system is installed.

7.3.2 Review and Update System and User Manuals

System and user manuals developed or updated during the Development and Test Phase are reviewed for accuracy and completeness and updated, as needed. Changes are incorporated to reflect modifications or enhancements that have been incorporated. Additional detail is incorporated to reflect the availability of new information.

7.3.3 Review and Update Project Planning Documentation

The Project Management Plan (PMP), Work Breakdown Structure (WBS), Risk Management Plan (RMP), Acquisition Plan, Project Risk Assessment, and Configuration Management (CM) Plan are updated in this phase, as needed. Any changes in project activities, schedules, or resource needs that may have occurred as a result of implementation planning and execution are incorporated into the appropriate planning documents (e.g. PMP, WBS, Acquisition Plan, CM Plan). Risk planning and assessment documents are updated to reflect closure of previously identified risks as well as newly identified risks.

7.3.4 Train Personnel

Users and operations personnel trained during this phase in accordance with the processes established in the Training Plan. The purpose is to fully acquaint them with the system and equip them for using the system effectively and efficiently. System and user manuals developed during the previous phase are utilized during the training sessions.

7.3.5 Perform Computer Security Certification and Accreditation

Computer Security Certification is the comprehensive analysis of the technical and non-technical security features and other safeguards of a system to establish the extent to which a particular system meets a set of specified security requirements. The certification process includes completing a Security Risk Assessment, System Security Plan, Security Operating Procedures, Security Test and Evaluation, and Certification Statements. All of these documents grouped together comprise the certification package. They are submitted to the Agency Computer Security Officer for review and approval. It is then submitted to the designated approval authority within the Office of the Chief Information Officer (OCIO).

Computer Security Accreditation is defined as a "formal declaration by an accrediting authority that a computer system is approved to operate in a particular security mode using a prescribed set of safeguards." The Designated Accrediting Authority (DAA) may be a senior manager of DOL or from within the Agency. The DAA will review the letter from the OCIO and the accompanying certification package. The DAA will determine, based on the remaining residual risk, if the system is operating in the best interest of DOL/Agency. After ensuring that all needs have been fulfilled, Computer Security Accreditation is granted.

7.3.6 Implement System

The Implementation plan, developed in the previous phase is reviewed. Incorporate changes as needed. Conduct a final system review. Install the system in the production environment, data is converted as needed, and sample testing is conducted to verify that the system operates correctly. System and user documentation is reproduced and distributed to appropriate personnel. An Implementation Certification is signed by the Project Manager and the System Owner to confirm that the system has been successfully implemented according to documented plans and procedures.

Successful implementation is ensured when known deficiencies and requirements are addressed and resolved before system implementation. Modifications made to the system both before and during implementation should be documented and provided to system users, operators, and other affected personnel. At the end of this phase, the product baseline (consisting of the production system, database(s), an updated data dictionary, and supporting documentation) is established.

7.4 Phase Deliverables

Deliverables produced and/or updated in the Implementation Phase are described below. Deliverables are reviewed and approved by the designated reviewing authority before the IT system moves to the next phase.

7.4.1 Core deliverables

Core deliverables are those that are required during this phase. The following core deliverables are initiated, or updated if they already exist, and finalized in the Implementation Phase.

- Computer Security Certification - The following four documents comprise the certification package. They must be submitted to the Agency Computer Security Officer for certification:

  a. A memorandum stating completion of security activities
  b. A Computer Security Certification Statement
  c. A Summary of Compliance
  d. A Statement of Residual Risk

  Sample outlines for the above documents are provided in Appendix F. See also FIPS Publication 102 and the DOL Computer Security Handbook, Appendix A and G.

- Security Accreditation Letter - Upon completion of the Computer Security Certification, the certification package (see above) and the Security Accreditation Letter are submitted by the OCIO Program Manager to the Designated Accrediting Authority (DAA) for review and approval. See FIPS Publication 102 Sections 2.5.2/2.6.2 and DOL Computer Security Handbook, Appendices A and G.

- Implemented System - Following successful completion of acceptance testing, the system is ready for implementation as a production system. The system is installed and verified in the production environment. Associated system and user manuals are turned over to the production staff and are carried forth into the Operations and Maintenance Phase.

- Trained Personnel - Users and operations training is conducted in accordance with the Training Plan.

- Implementation Certification Statement - This statement is signed by the Project Manager and the System Owner and verifies that the system has been successfully implemented according to documented plans and procedures. A sample outline for an Implementation Certification Statement is provided in Appendix F. See IEEE/EIA 12207.0-1996 Section 5.3.12.

7.4.2 Updated Deliverables

The following documents, generated and/or updated during previous SDLCM phases, may be updated or finalized during this phase. These are living documents that evolve throughout the life cycle and are updated, as needed, to a level of detail that reflects the maturity of the project.

- Risk Management Plan (RMP) - The RMP is updated during this phase to reflect project advances, reassessment of existing risks, and identification and assessment of new risks. It is essential that new risks identified during this phase (pertaining to implementation and future operations) are documented so that appropriate measures can be taken during the operations and maintenance phase to overcome or mitigate such risks. A sample format for a RMP is provided in Appendix B. See Clinger-Cohen Act 1996 Section 5122(a)(b)(5), OMB Director's Policy Memorandum M-97-02 (Raines Rules), IEEE/EIA 12207.0-1996 Section 5.1.1.6, NIST Handbook (March 1995), OMB A-130 Appendix III B, IEEE/EIA 12207.2-1997 Section 7.1.2.1(f)/ Annex L.

- Project Management Plan - The PMP is a core deliverable of Conceptual Planning, and is subsequently updated as the project advances and management has more information and additional time to improve the previous analysis and conclusions. Updating continues through four phases, into the Implementation Phase where it is finalized to reflect any changes in tasking, scheduling, or resources. A sample format for a PMP is provided in Appendix B. See IEEE/EIA 12207.2-1997 Section 5.2.4.2.

- Acquisition Strategy/Plan - The Acquisition Plan, produced during the Design Phase (See Chapter 5), is updated as needed, to address any changes needed for acquiring necessary hardware, software, telecommunication capabilities, and contractor support services. It supplements the Project Management Plan. A sample outline for an Acquisition Plan is provided in Appendix D. See OMB Director's Policy Memorandum M- 97-02 (Raines Rules), Clinger-Cohen Act 1996 Section 5124, OMB A-130 Appendix IV Section 8b(5), OMB A-109, IEEE/EIA 12207.0-1996 Sections 5.1.1.2, 5.1.1.8, and 5.2.4.

- Work Breakdown Structure (WBS) - The WBS supplements the Project Management Plan and is updated during this phase to reflect any planning and tasking changes that have been made to the PMP. Additional information for a WBS (e.g., Summary WBS, Project WBS, and Contract WBS) is provided in Appendix B. See IEEE/EIA12207.2-1997 Section 5.2.4.5 (c).

- Project Risk Assessment (PRA) - The Project Risk Assessment is updated during this phase to address the re-evaluation of previously identified risks as well as additional risks that may have been identified during implementation activities. This assessment may be a part of the RMP. See OMB A-130 Section 8 and Appendix III Ba2, IEEE/EIA 12207.0-1996

Section 5.2.4.5, and Clinger-Cohen Act 1996 Section 5131.

- System Security Plan (SSP)/Security Risk Assessment (SRA) - The SSP/SRA is a living, dynamic document reflecting the current posture of the IT system and should be initially developed in the Planning and Requirements Definition Phase and updated in later phases. It is updated in this phase to reflect system security considerations discovered during system implementation activities. It is also updated after a significant system configuration change, or at least once in every 3 years. See OMB A-130 Section 8 and Appendix III Ba2, IEEE/EIA 12207.0-1996 Section 5.2.4.5, Clinger-Cohen Act 1996 Section 5131, and DOL Computer Security Handbook.

- Configuration Management (CM) Plan - The CM Plan is updated in this phase, as needed, to support identification of, or changes to: the locations where configuration items are stored (electronically or hard copy); the automated libraries used to store other documentation; the software components of the system; and configuration audits that will be performed. See IEEE/EIA 12207.2-1997 Section 6.2, IEEE/EIA 12207.0-1996 Section 5.2.4.5, and ISO 10007.

- Systems Manuals - System Manuals are updated during this phase to reflect needed changes identified during system implementation activities. At the end of this phase, they should accurately document the design, development, production, distribution, operation, maintenance, and management of the IT system. This documentation is carried forward into the Operations and Maintenance Phase. See IEEE/EIA 12207.2-1997 Section 6.1.

- User Manuals - User Manuals are updated during this phase to reflect needed changes identified during system implementation activities. At the end of this phase, they should accurately document instructions, guidance, and reference information relating to user execution of the system. This documentation is carried forward into the Operations and Maintenance Phase. See IEEE/EIA 12207.2-1997 Section 6.1.

7.5 Phase Considerations

A number of project related decisions are made in this phase that may address the following questions:

- What changes are necessary to complete the system implementation?
- Is a process in place to allow for continued upgrade decisions such as:
  - What upgrades are required to address new or changing requirements?
  - What approvals are necessary to undertake the change?

- Are the appropriate resources and sufficient funding available to support approved system changes, upgrades, and new requirements?

Systems Development and Life Cycle Management (SDLCM)

8. OPERATIONS AND MAINTENANCE PHASE

8.1 Phase Overview

Once a system becomes operational, it moves to the Operations and Maintenance Phase. The emphasis of this phase is to ensure that user needs continue to be met and that the system continues to perform according to specifications. Routine hardware and software maintenance and upgrades are performed to ensure effective system operations. User training continues during this phase as needed to acquaint new users to the system or to introduce new features to the current users. Additional user support is provided as an ongoing activity to help resolve reported problems. This phase continues until the system is retired. Exhibit 8-1 identifies essential inputs, activities, and deliverables of this phase.

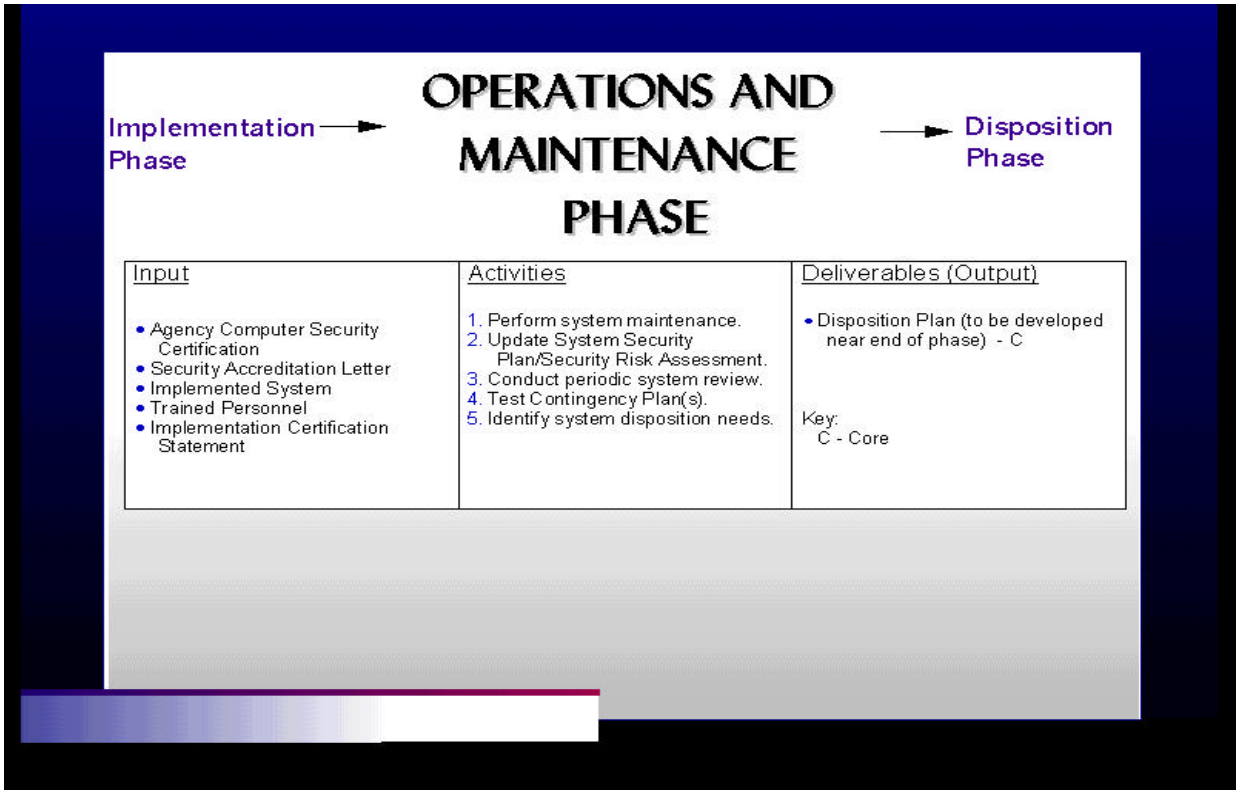


Exhibit 8-1: Operations and Maintenance Phase Deliverables, Activities, Deliverables

8.2 Phase Inputs

The essential inputs to the Operations and Maintenance phase are the core deliverables that were produced during the Implementation phase. They are:

- Agency Computer Security Certification signed off by the Project Manager and the System Owner
- Security Accreditation letter signed off by the Designated Accreditation Authority
- An Implemented System installed and operating in the production environment
- Trained personnel, along with associated training documentation
- Implementation Certification Statement

All deliverable documents produced in prior phases are turned over to system administrators, maintainers, and support personnel. Documentation is updated as needed utilizing established configuration management and control processes as system enhancements or changes are incorporated.

8.3 Phase Activities

8.3.1 Perform System Maintenance

System Maintenance encompasses a wide gamut of activities including routine activities such as backing up data and program files and upgrading/replacing hardware/software systems, application software, and vendor supplied COTS packages. Maintenance activities also involve fixing previously undetected errors. Various reviews may be conducted during this phase to gather important information used to assess continued use of the system, to evaluate additional enhancements, and to obtain user comments.

Maintenance personnel determine if modifications to the system and databases are needed to resolve errors, enhance system performance, or to provide new capabilities. New capabilities may take the form of routine maintenance or constitute enhancements to the system or database in response to user requests for new or improved capabilities. The Request for Information Technology Services (RITS) is the mechanism used to identify a need or opportunity to enhance a system or fix previously undetected errors.

Proposed changes are reviewed and approved by the appropriate review authority (as per the DOL Guide to IT Capital Investment Management) before implementation. Major system modifications or enhancements that are needed after the system has been implemented will follow the life cycle process from planning through implementation as appropriate. In this case a Project Management Plan including a Feasibility Study is updated or developed to identify needed modifications to the existing system and related documentation. The appropriate reviews and testing are conducted based on the scope of the modification. The maintenance manual is updated as needed to

document approved changes to the system.

8.3.2 Update System Security Plan/Security Risk Assessment

By the time the IT effort gets to this phase, all security activities should have been either initiated or completed. The System Security Plan (SSP)/Security Risk Assessment (SRA) is updated once every 3 years or when a significant change occurs (see DOL Computer Security Handbook). Computer and telecommunications security awareness training is provided to all personnel having access to DOL IT systems. The Project Manager must ensure that security-operating procedures are also kept updated. See OMB A-130 Section 8 and Appendix III Ba2, IEEE/EIA 12207.0-1996 Section 5.2.4.5, and Clinger-Cohen Act 1996 Section 5131, DOL Computer Security Handbook.

8.3.3 Conduct Periodic System Review

The Periodic System Review is conducted (at least annually) during this phase. This review is performed to evaluate system performance, user satisfaction with the system, adaptability to changing business needs, and new technologies that might improve the system. This review is diagnostic in nature and may lead to development or maintenance activities. See IEEE/EIA 12207.2-1997 Section 6.6 and Clinger-Cohen Act 1996 Section 5113 B4.

8.3.4 Test Contingency Plan(s)

Contingency plan(s) are tested during this phase. To the extent possible, all testing should be done by simulating actual conditions. Problems noticed during testing along with optimum solutions should be discussed and disseminated to appropriate parties as “Lessons Learned”. Contingency Plan(s) testing should be done at regular periodic intervals to create and maintain a sense of awareness and preparedness among Agency personnel of likely calamities that could occur.

8.3.5 Identify System Disposition Needs

Since the normal life cycle of an IT system is usually several years, disposition planning may not occur until the end of this phase (i.e., when a decision has been made to retire the IT system). However, if the system processes sensitive data and interfaces to other IT systems, it is advantageous to identify and document the system disposition plan and associated impacts in the early stages of the life cycle. This will ease the effort later in this phase when the final Disposition Plan is prepared.

8.4 Phase Deliverables

Deliverables produced and/or updated in the Operations and Maintenance Phase are described below. Deliverables are reviewed and approved by the designated reviewing authority before

the IT system can move to the next phase.

8.4.1 Core Deliverables

Core deliverables are those that are required during this phase. The following core deliverables are initiated during the Operations and Maintenance Phase:

- Disposition Plan – The objective of the Disposition Plan is to state the approach and processes for disposing of a system in a planned orderly manner and to ensure that the system is properly archived or incorporated into other systems. The Disposition Plan is initiated (or updated, as needed, if it already exists) in this phase. It is finalized once a decision has been made to retire the system, which may not occur until later in the phase. A sample outline for a Disposition Plan is provided in Appendix G. See IEEE/EIA 12207.0 – 1996 Section 5.5.6.

8.4.2 Updated Deliverables

The following documents generated during previous SDLCM phases may be updated during this phase. These are living documents that evolve throughout the life cycle and are updated as needed to a level of detail that reflects the maturity of the project.

- Risk Management Plan (RMP) – The RMP is reviewed to ensure that it reflects any maintenance activities that have occurred during this phase. It is possible that certain risks that were projected during the development phase may no longer be applicable or may need to be upgraded or downgraded depending upon the prevailing circumstances. In addition, due to the changing environment, new risks may have surfaced that may require additional means/measures for risk reduction. See Chapter 3 for a description of the Risk Management Plan. See Clinger-Cohen Act 1996 Section 5122(a)(b)(5), OMB Director's Policy Memorandum M-97-02 Raines Rules), IEEE/EIA 12207.0-1996 Section 5.1.1.6, NIST Handbook (March 1995), OMB A-130.

- Project Risk Assessment – During this phase, programmatic and technical risks associated with maintenance activities (e.g., hardware/software upgrades, personnel changes, IT system disposal, etc.) may need to be reassessed. The Project Risk Assessment may be part of the Risk Management Plan. See Chapter 4 for a description of the Project Risk Assessment. See Clinger-Cohen Act 1996 Section 5122(a)(b)(5), OMB Director's Policy Memo M-97-02 (Raines Rules), IEEE/EIA 12207.0-1996 Section 5.1.1.6, OMB A-130 Appendix III B, IEEE/EIA 12207.2-1997 Section 7.1.2.1(f)/ Annex L.

- System Security Plan (SSP)/Security Risk Assessment (SRA) – With the passage of time, information that was once considered of high security value may need to be declassified or have its classification downgraded. Advances in hardware technology may permit applications and software that were once encoded before transmission to be transmitted as

plain text code over a more secure network. To reflect this constantly changing pattern in hardware and software, SSP/SRA's are updated as needed. See Chapter 4 for a description of the System Security Plan/Security Risk Assessment. See OMB A-130 Section 8 and Appendix III Ba2, IEEE/EIA 12207.0-1996 Section 5.2.4.5, and Clinger-Cohen Act 1996 Section 5131 and DOL Computer Security Handbook.

- System Manuals – System manuals are updated to reflect any changes in hardware and software that may occur in the operating environment, application software or procedures for installing, operating or maintaining applications. See Chapter 6 for a description of System Manuals. See IEEE/EIA 12207.2-1997 Section 6.1.

- User Manuals – User manuals need to be updated to reflect changes in application software, databases, file layouts, operating procedures, etc. See Chapter 6 for a description of User Manuals. See IEEE/EIA 12207.2-1997 Section 6.1.

8.5 Phase Considerations

Key project approach considerations during this phase may address the following questions:

- How should the evaluation of the system/data be conducted?

- What new or additional user support activities are needed?

- What improvements in system/data functionality, quality, and performance are required?

- What adjustments are needed to the current system/data management procedures?

Project execution considerations include planning the required changes or enhancements to the system and determining if a particular enhancement should be implemented during this phase or cycled back through the SDLCM. These can be addressed by obtaining an answer to the following question:

- Does this change/enhancement need to be implemented during this phase or be cycled back through the SDLCM?

Planning now begins for the preservation of data in accordance with the records management and property disposal requirements of the Agency. This will include archiving/converting of the data to suit the new environment and eventual archiving of the software. The system planning activities preserve information about the current production system and the evolution of the system through its life cycle. The following question can be asked:

- Is a records management and property disposal process defined to address

archiving/conversion of software/data and disposal of hardware for the system under retirement?

Systems Development and Life Cycle Management (SDLCM)

9. DISPOSITION PHASE

9.1 Phase Overview

The Disposition Phase represents the end of the systems life cycle. It provides for the systematic termination of a system to ensure that vital information is preserved for potential future access and/or reactivation. The system, when placed in the Disposition Phase, has been declared surplus and/or obsolete, and is scheduled to be shut down. The emphasis of this phase is to ensure that the system (e.g. software, data, procedures, and documentation) is packaged and archived in an orderly fashion, enabling the system to be reinstalled later if desired. System records are retained in accordance with DOL policies regarding retention of electronic records. Exhibit 9-1 identifies essential inputs, activities, and deliverables of the Disposition Phase.

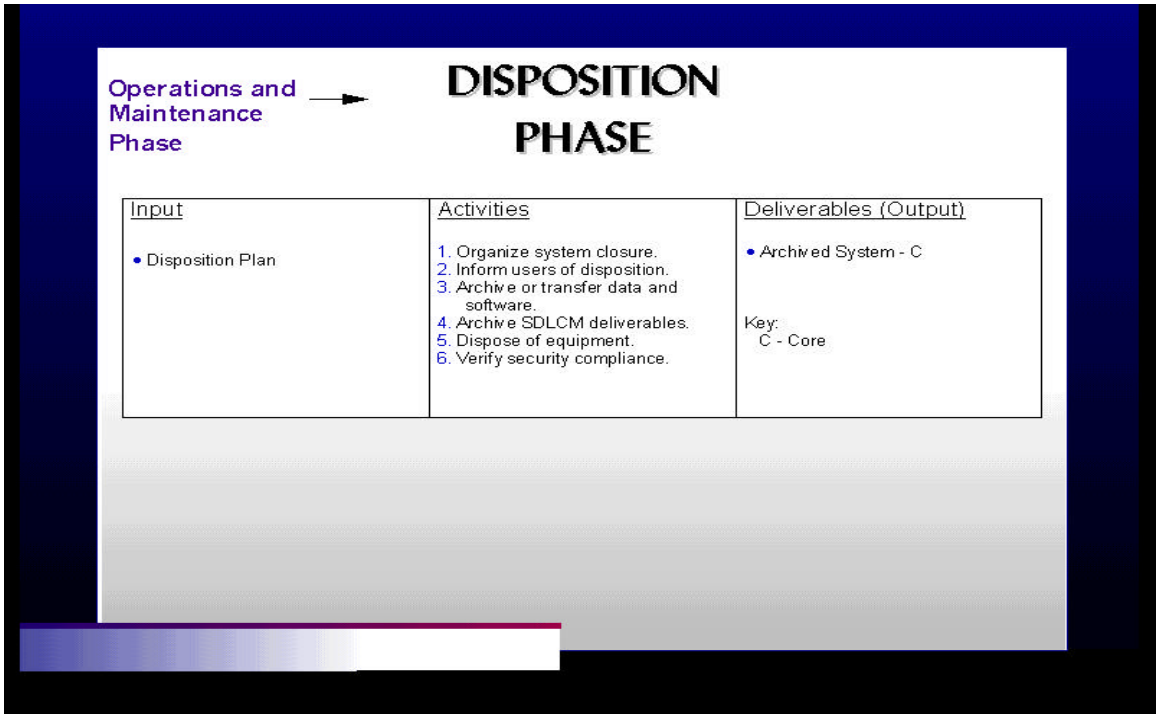


Exhibit 9-1: Disposition Phase Inputs, Activities, Deliverables

9.2 Phase Inputs

The key input to this phase is the core deliverable produced during the Operations and Maintenance Phase, the Disposition Plan. The Plan addresses all facets of archiving, transferring, and disposing of the system and the data. Particular emphasis is given to proper preservation of the data processed by the system so that it can be effectively migrated to another system or archived and restored in accordance with applicable record management regulations and policies. The Disposition Plan is executed during this phase and the system is retired in accordance with the documented processes.

9.3 Phase Activities

9.3.1 Organize System Closure

Initial disposition planning activities specified in the Disposition Plan are initiated. The schedule for system disposal is finalized and coordinated with involved parties. Specific activities for proceeding are defined and may include: identifying the software components to be preserved; identifying the data to be preserved; determining how the remaining equipment will be disposed of; and identifying what support life cycle products should be archived and the method for doing so.

9.3.2 Inform Users of Disposition

Users, operators, and maintainers of the system are notified of the plans for disposing the system. Ample time must be permitted for users to produce needed reports and/or archive specific information they may need to support their work activities.

9.3.3 Archive or Transfer Data and Software

Copies of code and data are archived to a designated environment specified in the Disposition Plan. Related system build, installation, and set-up scripts are archived so that the system may be reinstalled later. The system disposition activities preserve information not only about the current production system but also about the evolution of the system through its life cycle.

9.3.4 Archive SDLCM Deliverables

SDLCM life cycle documentation or deliverables are archived for future reference. This includes development information (e.g., requirements, design, and testing documents), planning information (e.g., implementation, risk management, implementation, disposition, and training plans), and information specifying how to use and operate the system (e.g., user and system manuals).

9.3.5 Dispose of Equipment

Retirement of IT systems may result in obsolete or excess equipment that needs to be either

disposed of or reallocated. Excess inventory is disposed of or reallocated, as needed, accordance with DOL policies and procedures.

9.3.6 Verify Security Compliance

As specified in the DOL Computer Security Handbook, the retirement of classified systems requires that documentation, software, and data are archived with appropriate security classifications. A determination needs to be made regarding how and when the termination of the system/data should be conducted.

9.4 Phase Deliverables

The only deliverable of the Disposition Phase is a system that has been archived in accordance with the procedures set forth in the Disposition Plan. The archived system is comprised of the packaged set of software, data, procedures, and documentation associated with the archived application. Additional information for this deliverable is provided in Appendix G. See IEEE/EIA 12207.2-1997 Section 5.5.6.1.

9.5 Phase Considerations

Key considerations during this phase may address the following questions:

- Have all potential future users of the system been notified of the archiving plan?
- Have all necessary code, data, and documentation been located?
- Is the means of preservation of the materials and their location considered secure?
- Will instructions for regeneration of the system be easy to find and understand?

Systems Development and Life Cycle Management (SDLCM)

APPENDIX A – ACRONYMS AND GLOSSARY OF TERMS

Acronym List

ADP	Automated Data Processing
BPR	Business Process Reengineering
CBA	Cost Benefit Analysis
CM	Configuration Management
COTS	Commercial-off-the-shelf
CSC	Computer Security Certification
CSO	Computer Security Officer
C&TS	Computer and Telecommunications Security
DAA	Designated Accrediting Authority
DOL	Department of Labor
FOIA	Freedom of Information Act
FRD	Functional Requirements Document
IRM	Information Resources Management/Information Resources Manager
IT	Information Technology
ITA	Information Technology Architecture

I-TIPS	Information Technology Investment Portfolio System
ITMRA	Information Technology Management Reform Act (AKA Clinger-Cohen Act 1996)
LAN	Local Area Network
MOU	Memorandum of Understanding
MRC	Management Review Council
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PM	Project Manager
PMP	Project Management Plan
POC	Point of Contact
PRA	Project Risk Assessment
QA	Quality Assurance
RD	Requirements Document
RITS	Request for Information Technology Services
RMP	Risk Management Plan
SCR	System Change Request
SDLCM	System Development and Life Cycle Management
SFA	System Fielding Authorization
SOW	Statement of Work
SRA	Security Risk Assessment
SSP	System Security Plan
ST&E	Security Test and Evaluation
TRB	Technical Review Board

WAN	Wide Area Network
WBS	Work Breakdown Structure

Glossary of Terms

Acquisition Plan – The plan that outlines how all the hardware, software, and other services will be acquired during the life of the project.

Change Control Documents – These documents may be used in the configuration management process to track, control, and manage the change of configuration items over the life cycle.

Computer Security Certification – Four documents that must be submitted to the OCIO Computer System Security Manager before implementation.

Configuration Management (CM) – The uniform practices that manage, establish, and change the system hardware and software.

Configuration Management Plan – The document that outlines the CM practices. The plan will identify which items need to be placed under configuration management, the methods for tracking and reporting changes, and where the items are stored.

Contingency Plan – The plan that documents how an entity will continue to operate in the event of a system failure.

Cost Benefit Analysis (CBA) – The analysis that provides the costs versus the benefits of implementing the various alternatives in a project. The purpose of the Cost Benefit Analysis Document is to provide managers, users, designers and auditors with adequate cost and benefit information to analyze and evaluate alternative approaches. This document, in conjunction with the Feasibility Study Document, should provide the information for management to make decisions to initiate or continue the development, procurement or modification of the project.

Customer The individual or organization who will use the project product.

Disposition Plan – A plan developed to end the operation of the system in a planned, orderly manner, and to ensure that system components and data are properly archived or incorporated into other systems.

Feasibility Study – A study to determine if a project is feasible, before expending resources. The purpose of the Feasibility Study Document is to provide: (1) an analysis of the objectives, requirements and system concepts; (2) an evaluation of alternative approaches for reasonably achieving the objectives; and (3) identification of a proposed approach. This document, in conjunction with the Cost Benefit Analysis Document, should provide management with adequate information to make decisions to initiate or continue the development, procurement or modification of the project.

Implementation Plan – The plan that explains how a completed system will be placed into production.

Information Resources Management/Information Resources Manager (IRM) – Manager at the Agency level who may assist the Project Owner in developing an initiative, especially during the early stages of implementation of the IT Capital Planning process.

Information Technology Investment Portfolio System (I-TIPS) An innovative web-based decision support and project management tool for managing IT investments. Additional information on I-TIPS can be found at I-TIPS at Online http://www.itips.gov.

Legacy Data Plan – This plan identifies the old data that cannot be processed by the new system. It also states the period of time that the data covers, and where it resides. It also discusses the old data that may have been converted.

Network Diagrams – Graphical representations of the relationships between tasks within a project and the dependencies that may affect schedule or resource requirements.

Office of the Chief Information Officer (OCIO) – Consists of the CIO and his/her staff. If the initiative is at the CIO level threshold, the OCIO is responsible for performing a due diligence review process and deciding the selection status of the initiative. The OCIO is also responsible for checking initiatives against cross-cutting exceptions. If the initiative is at the TRB/MRC level, the OCIO is responsible for working with the Project Owner to provide initiative information to the TRB and coordinating Agency presentations to the TRB/MRC.

Performing Organization The enterprise whose employees are most directly involved in doing the work of the project.

Periodic System Review – A review conducted at least annually, which evaluates the system performance, user satisfaction, adaptability to changing business needs, and new technologies.

Post-Implementation Review – A review which is conducted to ensure that the system functions as planned and expected, to verify that the cost is within estimates, and to verify that the intended benefits are derived.

Post-Termination Review – A report that details the findings of the post-disposition review.

Project Management Plan (PMP) – The overall plan of a project. This plan includes the various tasks, the schedule, the needed resources, and the measurement criteria to ensure that the project is proceeding as planned.

Project Manager (PM) – The person who has the overall responsibility for the management of the project. The project manager usually works with the System Owner to ensure that the project is meeting the needs and requirements of the System Owner.

Requirements Document (RD) – A formal statement of the application's business requirements, which may serve the same purpose as a contract.

Requirements Management Process – the process that establishes and maintains a common understanding between a customer (DOL agency or OCIO management) and the software development team and controls the establishment, prioritization, acceptance of, and changes to documented requirements.

Risk Assessment – The assessment documents the risk of the system and outlines potential impacts on the mission of the system due to loss or degradation of resources. It should also evaluate the effectiveness of protection of sensitive and critical applications.

Risk Management Plan – The plan that describes the various risks within a project. The plan includes how to control and mitigate the risks, and the likelihood of an action occurring.

Security Operating Procedures – A guidance document that provides users and administrators with detailed requirements on how to operate and maintain the system in a secure manner.

Security Test and Evaluation (ST&E) – The process of determining the adequacy of a system's security mechanisms in relation to completeness and correctness and the degree of consistency between system documentation and actual implementation.

Software Development Folder – This is the documentation that pertains to the development of each unit or module, including test cases, software, test results, approvals, and any other items that help to explain the functionality of the software.

Statement of Work (SOW) – This document outlines the scope of the work that is to be performed.

System Fielding Authorization – The agreement between the Project Manager, the System Owner, the data processing support staff, and the user, stating that the system meets with all known needs and that it has been developed and tested according to the provisions of the Project Management Plan and other SDLCM plans, and is acceptable for installation.

System of Record – The primary system that a department or agency is using to perform a specific task. The system must be recorded in the Federal Register. Included in the notice are the purpose of the system, the use of the system, the types of data the system contains, where the records are located, how the records are stored, and the identity of the System Manager.

System Owner – The person, or organization, which is sponsoring the project. The System Owner is responsible for insuring that resources are secured, including funding, personnel, and facilities.

System Security Plan – This plan documents the management of systems that contain sensitive information.

Technical Review Board (TRB) – Serves as the Department's first tier Investment Review Board for above threshold IT investments and a forum to identify and resolve Department-wide IT related issues. The TRB is responsible for scoring the initiatives and recommending an IT investment portfolio to the MRC. The TRB is chaired by the Deputy CIO and its members consist of IRM Managers and Administrative Officers (AOs) from each Agency.

Test Analysis Approval Determination – A document attached to the test analysis report. It summarizes the readiness of the software from migration to production.

Test Analysis Report – This report documents the testing of the software as it was defined in the test plan.

Test and Evaluation (T&E) – A process that verifies that a change to a model has been implemented correctly.

Test Plan – The document prepared to ensure that all aspects of the system have been tested and can be implemented.

Test Problem Reports – This report documents the problems that were encountered during testing.

Training Plan – This plan outlines the objectives, needs, strategy, and curriculum to be addressed when training the users on the new or enhanced system/application.

User Group – A group of people that provides subject matter expertise in the development of the project.

User Satisfaction Review – A review designed to provide responses on operational systems to help determine is the systems are accurate and reliable.

Work Breakdown Structure (WBS) – As part of the Project Management Plan, this structure ties the tasks to the specific phase of the life cycle along with the time requirements for each task within each phase of the life cycle, for accomplishment.

Systems Development and Life Cycle Management (SDLCM)

APPENDIX B – CONCEPTUAL PLANNING PHASE DELIVERABLES

Cost Benefit Analysis

A Cost Benefit Analysis (CBA) is a tool for providing valuable information to decision makers about the viability of initiating or continuing information technology (IT) system development projects. CBAs serve many purposes: (1) to compare cost and benefit information in dollar terms; (2) to assess the total effect of potential system benefits, both in dollar terms and in qualitative terms, over a defined life cycle; (3) to identify a feasible alternative that best meets program objectives; (4) to help determine a baseline for measuring if a system meets performance objectives; and (5) to provide critical information, such as performance and cost data, necessary in an ongoing investment management process to help plan, budget, and allocate scarce resources among competing priorities. Two sample outlines for a CBA are shown in Exhibits B-1 and B-2.

Sample Cost-Benefit Analysis Format 1(Traditional)

Cover Page
Table of Contents
Executive Summary
1. Overview
    1.1 Purpose
    1.2 Scope
    1.3 Methodology
    1.4 DOL Needs
    1.5 Background
    1.6 Architecture
    1.7 Expected Useful Life
2. Objectives and Performance Measures
    2.1 DOL Mission
    2.2 DOL Strategic Objectives and Performance Measures
    2.3 Program Objectives and Performance Measures
    2.4 Tactical Objectives and Performance Measures
    2.5 <System> Performance Measurement and the DOL Mission

3. Assumptions, Constraints, and Conditions
    - 3.1 Assumptions
    - 3.2 Constraints
    - 3.3 Conditions
4. Feasible Alternatives
    - 4.1 Alternative 1
        - 4.1.1 Assumptions, Constraints, and Conditions—Alternative 1
        - 4.1.2 Advantages and Disadvantages—Alternative I
    - 4.2 Alternative 2
        - 4.2.1 Assumptions, Constraints, and Conditions—Alternative 2
        - 4.2.2 Advantages and Disadvantages—Alternative 2
    - 4.3 Alternative N
5. Cost Analysis
    - 5.1 Cost Categories
    - 5.2 <System> Cost Analysis
6. Benefit Analysis
    - 6.1 Key Benefit Terms
    - 6.2 Tangible Benefits
        - 6.2.1 Tangible Benefit 1: <Name>
    - 6.3 Summary of Tangible Benefits
    - 6.4 Intangible Benefits
    - 6.5 Summary of Intangible Benefits
7. Comparison of Costs and Benefits for <System>
    - 7.1 Results of the Comparison for <System>: Tangible Benefits
    - 7.2 Results of the Comparison for <System>: Intangible Benefits
    - 7.3 Conclusion
8. Sensitivity Analysis
    - 8. l Key Sources of Uncertainty
    - 8.2 Sensitivity Results
9. Results of the Analysis
    - 9.1 Results
        - 9.1.1 Alternative 1: <Name>
        - 9.1.2 Alternative 2: <Name>
        - 9.1.3 Alternative N: <Name>
10. Implementation Schedule
    - 10.1 Schedule
11. References and Documentation
    - 11.1 Documentation
    - 11.2 Interviews
12. Glossary and Acronyms
    - 12.1 Glossary
    - 12.2 Acronyms

Exhibit B-1: Sample Cost-Benefit Analysis Format 1 Outline

Sample Cost-Benefit Analysis Format 2 (Alternative)

Cover Page

Table of Contents

Executive Summary

1. Overview
   - 1.1 Purpose
   - 1.2 Scope
   - 1.3 Methodology
   - 1.4 DOL Needs
   - 1.5 Background
   - 1.6 Architecture
   - 1.7 Expected Useful Life
2. Objectives and Performance Measures
   - 2.1 DOL Mission
   - 2.2 DOL Strategic Objectives and Performance Measures
   - 2.3 Program Objectives and Performance Measures
   - 2.4 Tactical Objectives and Performance Measures
   - 2.5 <System> Performance Measurement and the DOL Mission
3. Assumptions, Constraints, and Conditions
   - 3.1 Assumptions
   - 3.2 Constraints
   - 3.3 Conditions
4. Cost Analysis
   - 4.1 Cost Categories
   - 4.2 <System> Cost Analysis
5. Benefit Analysis
   - 5.1 Key Benefit Terms
   - 5.2 Tangible Benefits
     - 5.2.1 Tangible Benefit 1: <Name>
     - 5.2.2 Tangible Benefit 2: <Name>
   - 5.3 Summary of Tangible Benefits
   - 5.4 Intangible Benefits
   - 5.5 Summary of Intangible Benefits
6. Comparison of Costs and Benefits for <System>
   - 6.1 Results of the Comparison for <System>: Tangible Benefits
   - 6.2 Results of the Comparison for <System>: Intangible Benefits
   - 6.3 Conclusion
7. Sensitivity Analysis
   - 7.1 Key Sources of Uncertainty
   - 7.2 Sensitivity Results
8. Results of the Analysis
   - 8.1 Results
   - 8.2 Conclusion
9. Implementation Schedule
   - 9.1 Schedule
10. References and Documentation
    - 10.1 Documentation
    - 10.2 Interviews

11. Glossary and Acronyms
    11.1 Glossary
    11.2 Acronyms

Exhibit B-2: Sample Cost-Benefit Analysis Format 2 Outline

Feasibility Study

The feasibility study describes the information management, business requirement, or opportunity in clear, technology-independent terms on which all affected organizations can agree. An information management requirement or opportunity can be prompted by such factors as new legislation, changes to regulations, or the growth of a program beyond the support capability of existing systems.

The feasibility study provides an overview of a complex business requirement or opportunity and determines if feasible solutions exist before full life cycle resources are committed. The requirement or opportunity is assessed in terms of technical, economic, and operational feasibility. The study contains decision criteria, comparisons of general solution possibilities, and a proposed solution. The study is conducted any time a broad analysis is desired before commitment of development resources.

A Cost Benefit Analysis (CBA) is prepared as a companion document with the feasibility study. The CBA is the document that provides managers with adequate cost and benefit information to analyze and evaluate alternative approaches. It provides information for management to make decisions to initiate a proposed program—to continue or discontinue the development, acquisition, or modification of information systems or resources.

A sample outline for a feasibility study is provided in Exhibit B-3.

Sample Feasibility Study Outline

Cover Page
Table of Contents
1. Introduction
  1.1 Origin of Request
    Identifies the originator and describes the circumstances that precipitated this project request. Provides the objectives of the feasibility study in clear, measurable terms.

  1.2 Explanation of Requirement
    Describes the information management requirement in programmatic, technology-independent terms. Should state the specific deviations from the desired situation and the source and/or cause of the new requirement or opportunity. Describes any new information need(s) associated with the requirement or opportunity. Should identify the cause(s) and effect(s) of the requirement or opportunity and validate the description of the requirement or opportunity with all affected organizations.

1.3 Organization Information

Identifies the organization(s) mentioned in Section 1.1, Origin of Request, and the pertinent current procedures, information, and systems of those organizations. Provides descriptions of the relevant procedures and systems as appropriate. Should specify all organizational units involved, list the organizational unit(s) at all levels of the DOL and external organizations that relate to the requirement or opportunity, and describe the pertinent mission area(s) and programmatic functions of each.

2. Evaluation Criteria

States the criteria by which the alternatives will be evaluated. The criteria should make a distinction among characteristics that must be present in the system for it to be acceptable.

3. Alternative Descriptions

Provides a description for each alternative proposed to handle the defined problem. Should describe the resources required; associated risk, system architecture, technology used, and the manual process flow for each alternative. Should state at least two alternatives for each feasibility study—one being the alternative of doing nothing—and predict the anticipated benefits of each alternative and the likely effects of not taking action on the alternative. Should also state benefits in terms of technical, operational, and economic feasibility.

3.1 Alternative Model

Presents a high-level data flow diagram and logical data model, if possible, from current physical processes and data for the proposed system alternative.

3.2 Description

States the required and desirable features, and provides a concise narrative of the effects of implementing this alternative.

4. Alternative Evaluation

A systematic comparison of the alternatives and documents potential problems resulting from the implementation of each.

5. Recommendation

A narrative that supports the recommended alternative. Should select the most advantageous alternative to implement the required functional capabilities based on the functional and technical concepts that satisfy the need. The information system should not be obtained at the price of inappropriate development risk or the loss of efficiency, capability, or capacity in the supported function.

Glossary

Exhibit B-3: Sample Feasibility Study Outline

Risk Management Plan

Risk Management (RM) refers to the assessment of potential outcomes of a project and the likelihood that one or more unsuccessful project outcomes may result. It also refers to the process of accepting, transferring, or mitigating risk. The Risk Management Plan (RMP) documents and identifies project risks; the analysis, assessment, and prioritization of those project risks; and lays out plans to implement actions to reduce the project risks throughout the project's life cycle. The

plan provides a control mechanism to monitor, report, and direct all risk mitigation activities. The RMP is initiated during the Conceptual Planning Phase and is updated and revised during the subsequent phases up to, and including, the Operations and Maintenance Phase. A sample outline of an RMP is shown in Exhibit B-4.

Sample Risk Management Plan Outline

Cover Page
Table of Contents

1. Introduction
   1.1 Purpose
   A clear, concise statement of the purpose of the RMP. Include the name and code name of the project, the name(s) of the associated system(s), and the identity of the organization that is responsible for writing and maintaining the RM plan.

   1.2 Background
   Describes the history of the project and the environment in which the project will operate. (This information may be included through reference to other project deliverable documents.) Includes identification of other systems with which the subject system interfaces; contractor support for development and maintenance; number of sites; system architecture, operating system, and application languages; and development methodology and tools used for the project.

   1.3 Scope
   A definitive statement of the scope of the risk management planning contained in this document, including the limits and constraints of the RMP.

   1.4 Policy
   Policy decisions that affect how risk management is conducted. May include requirements driven by legislative action or broad objectives of DOL or the project. Refer to the statement of work (SOW) and client interviews, for example, to determine what policy decisions have effect on the RMP.

   1.5 Reference Documents
   Lists documents that are referenced to support the risk management process. Include any project or standards documents that are referenced in the body of the plan or that have been used in the development of the document.

   1.6 Glossary

2. Risk Identification List
   List of risks. The risk identification list is used from the beginning of the project and is a major source of input for the risk assessment activity. Use the risk identification list throughout the life-cycle phases to ensure that all risks are properly documented.

3. Risk Assessment
   The Project Management Plan and the risk identification list are inputs to the risk assessment. Document results of the risk assessment in this section. The risk identification list should be

divided into two sections: external risks and internal risks. Internal risks are those that you can control. External risks are events over which you have no direct control. Each risk should be scored with an evaluation tool category such as 0 for "no risk," up to 5 for "very serious risk."

4. Risk Prioritization
   The results of prioritizing the risks. Prioritize the risk items from high to low based on the probability and impact analysis assessment from the previous section. If the evaluation tool of 0 to 5 was used from the previous section, then all the 5s (risk exposure threatens failure of the project) would be listed first, then the 4s, on down to the 0s.

5. Risk Action Plan
   Identifies and describes in detail the actions that will be taken to transfer or mitigate risks that are prioritized as high in Section 4. These actions should ultimately result in the reduction of project risk and should directly affect the Project Management Plan and the metrics used for the project.

Exhibit B-4: Sample Risk Management Plan Outline

Project Management Plan (PMP)

The Project Management Plan (PMP) is prepared for all projects. It is one of several essential project-planning documents that use a building-block approach to planning. It is a vehicle for documenting project scope, tasks, schedule, allocated resources, and interrelationships with other projects. It also provides details on the involved Agency units, required job tasks, and milestone and review scheduling.

Revisions to the PMP occur at the end of each phase and as information becomes available. Software tools designed for work breakdown structures (WBSs), Gantt charts, network diagrams, and activity detail reports are available and should be used to complete the PMP. The size of the PMP should be commensurate with the size and complexity of the systems development effort. A sample outline for a PMP is shown in Exhibit B-5.

Sample Project Management Plan

Cover Page
Table of Contents

1. Introduction
   Description of the Project Management Plan purpose and scope.

1.1 Project Description
   Description of the project in as much detail as is required to understand the nature of the project. Identify the project name and code, state the project's objective(s), and give the date the plan was finalized in the Conceptual Planning Phase.

1.2 Project Background

Describes why the project is important to the organization, its mission, and the capabilities the project will provide to the organization. Include any background or history that is important to understanding the project.

1.2.1 Project Development Strategy

An overview of the development strategy (work pattern) selected for the project. For example, this strategy might include prototyping the system, use of commercial off-the-shelf software, or conversion of an existing system from one hardware and software family to another.

1.2.2 Organization of the Project Management Plan

Describes the organization of the Project Management Plan.

1.3 Points of Contact

Identifies the key points of contact for the Project Management Plan, including the Project Owner and Project Manager. Identify any additional points of contact.

1.4 Project References

A bibliography of essential project references and deliverables produced before this point. For example, these references might include cost benefit analyses, existing documentation describing internal processes, or existing documentation of the system if the project is a conversion.

1.5 Glossary

This section provides a glossary of all terms and abbreviations used in the plan. If the glossary is several pages in length, include it as an appendix.

2. Organization and Responsibilities

The various organizations and staff titles, roles, and responsibilities involved in the IT project. Describe team structures, reporting responsibilities, relationships, and guidelines for status reporting internally and externally for any contractor support. Also, provide a roles and responsibilities matrix. Identify the following key organization components: organization owner for the project; manager responsible for the day-to-day administration of the project (if different from the owner); Quality Assurance (QA) organization; Configuration Management (CM) organization.

3. Project Description, Schedule, and Resources

List of all tasks/activities to be completed within each phase of the project. If possible, use diagrams and tables (automated tools) to list the tasks and show any possible relationships among them. Repeat any subsection for each known task within the project. Should provide a detailed description of each task and its schedule, budget, and management. Also, include an estimate of each software development phase-related work effort and deliverables. Note: The actual structure of this subsection may be organized as best suits the project.

3.1 Project Work Breakdown Structure

Description of the WBS required for the project. The WBS is a family-tree structure that relates to products produced and tasks performed at the various phases of the project life cycle. A WBS displays and defines the product(s) to be developed or produced and relates the elements of work (tasks) to be accomplished to each other and to the end product(s). Typically, three levels of WBSs are developed during the system development process: Summary, Project, and Contract. A WBS Dictionary is also helpful for creating and recording the WBS elements.

3.1.1 Summary Work Breakdown Structure

Description of the Summary WBS, a high-level WBS that covers the first three levels of the Project WBS. The Summary WBS is used for management presentations but is not used for detailed day-

to-day project management. The structure of the Summary WBS may vary depending on the nature of the project.

3.1.2 Project Work Breakdown Structure

Description of the Project WBS, the detailed WBS that is used for the day-to-day management of a project. The Project WBS includes all important products and work elements or tasks of the project, regardless of whether these tasks are performed by a DOL component or by a contractor. The Project WBS may be modified, if necessary, during the life cycle.

3.1.3 Contract Work Breakdown Structure

Description of the Contract WBS (CWBS), a further breakdown of the contract-specific WBS that covers the products and work elements or tasks from the Project WBS that will be performed by a subcontractor. In addition to items derived from the Project WBS, the CWBS includes contractor-specific items that may not be reflected in the Project WBS. Depending on the nature of the project, the subcontractor may be responsible for a given part of the project development activities (such as QA), for a specific part of the development life cycle (such as the Planning and Requirements Definition Phase), or for the entire development process. A preliminary CWBS may be specified in the acquisition plan. The contract line items, configuration items, contract work statement tasks, contract specification, and contractor responses will typically be expressed in terms of the preliminary CWBS.

3.1.4 Work Breakdown Structure Dictionary

A WBS Dictionary provides detailed descriptions of each WBS element. Each WBS Dictionary entry should contain the title of the WBS element it amplifies; a narrative describing the work represented by the element; the effort required (in person hours); the most likely duration (in calendar days); and references to any special skills or resources required to accomplish the work. WBS Dictionary entries should be completed only for the lowest-level WBS elements.

3.2 Resource Estimates

Estimate, for each WBS element, the total amount of human resource effort required, by resource category. Use available tools to estimate, store, and output resource requirements per WBS element to use in the next component of the PMP.

3.3 Schedule

The project schedule. Assumptions made about task duration, resource availability, milestones, constraints, and optimization criteria should be carefully documented. Provide the schedule in the forms of Gantt charts, milestone tables, and deliverables and dates lists.

3.4 Resource Acquisition Plan

Description of the addition (and eventual departure) of project resources via a resource acquisition plan. Each type of resource should be considered in this resource acquisition plan. The plan should specify the source of the resources, the numbers of each, the start date for each, and the duration needed. It also should consider additional, associated resource requirements, such as space, hardware and software, office equipment, other facilities, and tools.

3.5 Communication Plan

Discussion of frequencies, target audiences, media, sources, formats, locations, forms, and types of information delivered in each form of communication. Careful thought should be given to satisfying existing standards and following existing conventions, and consideration should also be given to improving the communication process in general and to ensuring that communication is enabled and simplified for all project team members and external entities. Periodic status reports, newsletters, bulletins, problem reports, issue lists, status and review meetings, team meetings, and other forms of communication should all be carefully considered and documented when creating the

communication plan. Output the communication plan in the form of a communication item/audience matrix.

3.6 Project Standards and Procedures

Technical standards, business-related standards, and QA standards. Technical standards and procedures include such things as naming conventions, walk-through requirements, CM rules, security standards, documentation requirements, tools, modeling techniques, and technical contractual obligations. Business-related standards and procedures include such things as procedures for scope changes, requirements changes, costing, and sign-off standards. QA standards and procedures include such things as review processes, testing procedures, and defect tracking requirements. QA may also provide standards on the use of metrics. Produce the project standards and procedures by making entries in the project workbook.

3.7 Risk Management

Address approaches for mitigating the effects of these factors. Add subsections as necessary to separate different categories of risk or different risk-inducing factors. Include plan here, or reference separate Risk Management Plan document (also in this appendix) also created during the Conceptual Planning Phase.

4. Security and Privacy

Address security and privacy requirements for the project and should ensure that the Project Management Plan reflects these requirements.

4.1 Privacy Issues

Identify privacy issues that should be addressed during the phases of the IT system effort and define the process to be established for addressing the privacy issues throughout the life cycle. (See DOL Computer Security Handbook). It is important that there be a preliminary analysis of the potential privacy effects of the proposed information system. The purpose will be to establish for the project team and the review process an awareness of the privacy-related issues that will have to be addressed as the system is planned, developed, and implemented.

4.2 Computer Security Activities

Review and evaluation of requirements for security risk assessment and computer security planning to determine that all system vulnerabilities, threats, risks, and privacy issues will be identified and that an accurate determination will be made of the sensitivity of the system and information.

Exhibit B-5: Sample Project Management Plan Outline

Systems Development and Life Cycle Management (SDLCM)

APPENDIX C – PLANNING AND REQUIREMENTS DEFINITION PHASE DELIVERABLES

Functional Requirements Document

The Functional Requirement Document (FRD) is formal statement of an application's business requirements. It serves the same purpose as a contract. The developers agree to provide the capabilities specified. The client agrees to find the product satisfactory if it provides the capabilities specified in the FRD. The FRD has the following characteristics:

- It demonstrates that the application provides value to DOL in terms of the business objectives and business processes in the 5-year strategic plan.
- It contains a complete set of requirements for the application. It leaves no room for anyone to assume anything not stated in the FRD.
- It is solution independent. The FRD is a statement of what the application is to do, not of how it works. The FRD does not commit the developers to a design. For that reason, any reference to the use of a specific technology is entirely inappropriate in an FRD.

A sample outline for an FRD is provided in Exhibit C-1.

Sample Functional Requirements Document Outline

Cover Page
Table of Contents

1. Introduction
  1.1 Project Description
    Provide a brief overview of the project.
    1.1.1 Background
      Summarize the conditions that created the need for the application.
    1.1.2 Purpose
      Describe the business objectives and business processes from the cost-benefit analysis (CBA) that this application supports.

1.1.3 Assumptions and Constraints

Assumptions are future situations, beyond the control of the project, whose outcomes influence the success of a project (e.g., availability of a hardware/software platform; pending legislation; court decisions that have not been rendered; future trends in DOL missions; developments in technology). Constraints are conditions outside the control of the project that limit the design alternatives (e.g., Government regulations; standards imposed on the solution; strategic decisions). Be careful to distinguish constraints from preferences. Constraints exist because of real business conditions. Preferences are arbitrary. For example, a delivery date is a constraint only if there are real business consequences that can happen as a result of not meeting the date. For example, if failing to have the subject application operational by the specified date places the DOL in legal default, the date is a constraint. A date chosen arbitrarily is a preference. Preferences, if included in the RD, should be noted as such.

1.1.4 Interfaces to External Systems

Name the applications with which the subject application must interface. State the following for each such application: name of application; owner of application (if external to the DOL); details of interface (only if determined by the other application).

1.2 Points of Contact

List the names, titles, and roles of the major participants in the project. At a minimum, list the following: DOL project leader; development project leader; user contacts; DOL employee whose signature constitutes acceptance of the FRD.

1.3 Document References

Name the documents that were sources of this version of the RD. Include meeting summaries, white paper analyses, CBA, and other Systems Development and Life Cycle Management deliverables, as well as any other documents that contributed to the RD. Include the Configuration Management identifier and date published for each document listed.

2. Business Requirements

The business requirements describe the core functionality of the application. This section includes the data and process requirements.

2.1 Data Requirements

Describe the data requirements by producing a logical data model, which consists of entity relationship diagrams, entity definitions, and attribute definitions. This is called the application data model. The data requirements describe the business data needed by the application system. Data requirements do not describe the physical database.

2.2 Process Requirements

Process requirements describe what the application must do. Process requirements relate the entities and attributes from the data requirements to the users needs. State the functional process requirements in a manner that enables the reader to see broad concepts decomposed into layers of increasing detail.

3. Operational Requirements

Operational requirements describe the non-business characteristics of an application. State the requirements in this section. Do not state how these requirements will be satisfied. For example, in the Reliability section, answer the question, "How reliable must the system be?" Do not state what steps will be taken to provide reliability. Distinguish preferences from requirements. Requirements are based on business needs. Preferences are not.

3.1 Security

The Security section describes the need to control access to the data. This includes controlling who may view and alter application data.

3.2 Audit Trail

List the activities that will be recorded in the application's audit trail. For each activity, list the data to be recorded.

3.3 Data Currency

Data currency is a measure of how recent data are. This section answers the question, "When the application responds to a request for data how current must those data be?" Answer that question for each type of data request.

3.4 Reliability

Reliability is the probability that the system will be able to process work correctly and completely without being aborted. State the following in this section: damage that could result from this system's failure; minimum acceptable level of reliability; required reliability.

3.5 Recoverability

State the ability to restore functions and data in case of a failure.

3.6 System Availability

System availability is the time when the application must be available for use. Required system availability is used in determining when maintenance may be performed. In this section state the hours during which the application is to be available to users. Include the times when usage is expected to be at its peak. These are times when system unavailability is least acceptable.

3.7 Fault Tolerance

Fault tolerance is the ability to remain partially operational during a failure. Describe the following in this section: which functions need not be available at all times; if a component fails what (if any) functions must the application continue to provide; and what level of performance degradation is acceptable. For most applications, there are no fault tolerance requirements. When a portion of the application is unavailable, there is no need to be able to use the remainder of the application.

3.8 Performance

Describe the requirements for the following: Response time for queries and updates; throughput; expected volume of data; and expected volume of user activity (for example, number of transactions per hour, day, or month).

3.9 Capacity

List the required capacities and expected volumes of data in business terms. For example, state the number of cases about which the application will have to store data; state capacities in terms of the business. Do not state capacities in terms of system memory requirements or disk space.

3.10 Data Retention

Describe the length of time the data must be retained.

4. Requirements Traceability Matrix

The requirements traceability matrix (RTM) provides a method for tracking the functional requirements and their implementation through the development process. Each requirement is included in the matrix along with its associated section number. As the project progresses, the RTM is updated to reflect the status of each requirement. When the product is ready for system testing, the matrix lists each requirement, what product component addresses it, and what tests verify that it is correctly implemented. Exhibit C-2 illustrates a sample RTM.

5. Concepts of Operations (CONOPS)

A concept of operations (CONOPS) is required for all new systems or major system development efforts. A CONOPS is also required for all system enhancement efforts that will significantly affect current operational procedures and processes, or that affect more than a single system. The user group develops CONOPS, includes DOL Operational Experts, Managers, Subject Matter Experts, and System Owners. CONOPS must be consistent with applicable Federal law, Congressional direction and initiatives, the President's priorities, DOL Strategic Plans and Mission Statements.

5.1 Definition of Features

This section describes the features of the system.

5.2 Description of Operations
This section describes all aspects of the operations of the proposed system.
5.3 User Organization View
This section provides an explanation of how the system will look to each user organization.
5.4 Effect on Operations and Personnel
This section describes the effect of the system on personnel and on their operations.
5.5 Effect on Existing Operations
This section describes the effect of the system on existing operations.
5.6 Interfaces to Other Systems
This section describes the interfaces to other systems that will be built into the proposed new system.
5.7 Methods of Implementation
This section describes the intended implementation approach, from the users point of views.
5.8 Figure (Optional)
This optional section contains a graphical representation of CONOPS.

Exhibit C-1: Sample Functional Requirements Document Outline

Requirements Traceability Matrix

The requirements traceability matrix (RTM) provides a method for tracking the functional requirements and their implementation through the development process. It is may be part of the Functional Requirements Document (see Exhibit C-1, Section 4), or produced separately Exhibit C-2 illustrates a sample RTM.

Functional Requirement		***Verification Method**				**Test Plan Reference**
Description	**Para. Reference**	**A**	**I**	**D**	**T**	**Test Plan Reference**
The functionality of the Enhanced Primary Verification Process will be an expansion of the functionality of the point of sale (POS) emulation logic that is currently in place to support primary verification queries to ASVI.	3.2-01				X	TC 2.3.1.6
The 200 employers who will be part of the Phase II TVS Pilot will submit data electronically via an interface with the ASVI system.	3.2-02				X	TC 2.3.1.6
All secondary information will be passed electronically to the LA FCO from ASVI for secondary verification.	3.2-03				X	TC 2.3.1.10
After a determination has been made on a case, the status verifier will then send the response back to the employer electronically; the return path is the exact opposite of the preceding path to the FCO.	3.2-04				X	TC 2.3.1.10
The new system will be capable of tracking information on each case throughout both the						TC 2.3.1.6, 2.3.1.7,

Functional Requirement		***Verification Method**				**Test Plan Reference**
Description	**Para. Reference**	**A**	**I**	**D**	**T**	**Test Plan Reference**
primary and secondary verification processes.	3.2-05				X	2.3.1.11

A = ANALYSIS I = INSPECTION D = DEMONSTRATION T = TEST

Exhibit C-2: Sample Requirements Traceability Matrix

Systems Development and Life Cycle Management (SDLCM)

APPENDIX D – DESIGN PHASE DELIVERABLES

Acquisition Plan

The Acquisition Plan (AP) is a document that shows how all hardware, software, and telecommunications capabilities, along with contractor support services, are acquired during the life of the project. The AP helps ensure that needed resources are available at the time they are needed. The plan includes a milestone schedule that lists activities for completion and deliverables to be produced with appropriate estimated completion dates. A sample outline for an Acquisition Plan is shown in Exhibit D-1.

Sample Acquisition Plan Outline

Cover Page
Table of Contents
1. Background and Objectives
   1.1 Statement of Need
   This section introduces the plan with a brief statement of need. This section should discuss feasible acquisition alternatives and any related in-house efforts.
      1.1.1 Acquisition History
      1.1.2 Feasible Acquisition Alternatives Applicable Conditions

   1.2 Applicable Conditions
   This section states all the significant conditions affecting the acquisition, including requirements for compatibility with existing or future systems or programs and any known cost, schedule, and capability or performance constraints.

   1.3 Cost
   This section sets forth the established cost goals for the acquisition and the rationale supporting them, and discusses related cost concepts to be employed, as indicated in the subsequent sections.

      1.3.1 Life Cycle Cost
      This section discusses how the life cycle cost will be considered. If life cycle cost is not used, this section explains why. This section also discusses, if appropriate, the cost model used to develop the life cycle cost estimates. Life cycle cost is the total cost to the Government of acquiring, operating, supporting, and disposing of the items being acquired.

1.3.2 Design-to-Cost

This section discusses the design-to-cost objectives and the underlying assumptions, including the rationale for quantity, learning curve, and economic adjustment factors. It describes how objectives are to be applied, tracked, and enforced, and indicates the specific related solicitation and contractual requirements to be imposed. Design-to-cost is a concept that establishes cost elements as management goals to achieve the best balance between life cycle cost, acceptable performance, and schedule. Under this concept, cost is a design constraint during the Design and Development and Test Phases, and a management discipline throughout the acquisition and operation of the system or equipment.

1.3.3 Application of Should-Cost

This section discusses the application of should-cost analysis to the acquisition, as per FAR 15.810.

1.4 Capability or Performance

This section specifies the required capabilities or performance characteristics of the products being acquired, and states how they are related to the need.

1.5 Delivery or Performance-Period Requirements

This section describes the basis for establishing delivery of performance-period requirements, and explains and provides reasons for any urgency resulting in concurrency of development or justifying other than full and open competition.

1.6 Trade-Offs

This section discusses the expected consequences of trade-offs among the various costs, capability, performance, and schedule goals.

1.7 Risks

This section discusses the technical, cost, and schedule risks and describes what efforts are planned or underway to reduce the risk and the consequences of failure to achieve goals. The effects on cost and schedule risks imposed by concurrency of development and production should be discussed, if applicable.

1.8 Acquisition Streamlining

This section is included if the acquisition has been designated as part of a program subject to acquisition streamlining. It discusses plans and procedures to encourage industry participation via draft solicitations, pre-solicitation conferences, and other means of stimulating industry involvement during design and development. It also discusses plans and procedures for selecting and tailoring only the necessary and cost-effective requirements, and it states the timeframe for identifying which specifications and standards, that had originally been provided for guidance only, are scheduled to become mandatory.

2. Plan of Action

2.1 Sources

This section indicates the prospective sources of products that can meet the need. It considers the required sources, including consideration of small businesses, small disadvantaged businesses, and women-owned small business concerns. It addresses the results of market research and analysis and indicates their effect on the various elements of the plan.

2.2 Competition

This section discusses the source selection procedures for the acquisition, including the timing for submission and evaluation of proposals, and the relationship of evaluation factors to the attainment of the acquisition objectives.

2.3 Source-Selection Procedures
This section discusses the source selection procedures for the acquisition, including the timing for submission and evaluation of proposals, and the relationship of evaluation factors to the attainment of the acquisition objectives.

2.4 Contracting Considerations
This section discusses, for each contract contemplated, selection of the contract type; the use of multi-year contracting; options; or other special contracting methods; any special clauses, special solicitation provisions, Federal Acquisition Register (FAR) deviations required; if sealed bidding or negotiation will be used, and why; if equipment will be acquired by lease or purchase, and why; and any other contracting considerations.

2.5 Budgeting and Funding
This section explains, in accordance with FAR Part 11, the choice of product description types to be used in the acquisition.

2.6 Product Descriptions
This section explains, in accordance with FAR Part 11, the choice of product description types to be used in the acquisition.

2.7 Priorities, Allocations, and Allotments
This section specifies the method for obtaining and using priorities, allocations, allotments, and the reasons for them, in cases where the urgency of the requirement dictates a short delivery or performance schedule.

2.8 Contractor Versus Government Performance
This section addresses the consideration given to Office of Management and Budget (OMB) Circular A-76. Circular A-76 indicates that it is the policy of the Government to rely generally on private commercial sources for supplies and services, when certain criteria are met, while recognizing that some functions are inherently governmental and must be performed by Government personnel. It also considers relative cost when deciding between Government performance and performance under contract.

2.9 Inherently Governmental Functions
This section addresses the considerations given to Office of Federal Procurement Policy Letter 92-1. Inherently governmental functions are those functions that, as a matter of policy, are so intimately related to the public interest as to mandate performance by Government employees.

2.10 Management Information Requirements
This section discusses the management systems that will be used by the Government to monitor the contractor's effort.

2.11 Make-or-Buy
This section discusses considerations given to make-or-buy programs, as per FAR 15.7.

2.12 Test and Evaluation
This section describes the test program of the contractor and the Government. It describes the test program for each major phase of a major system acquisition. If concurrent development/deployment is planned, this section discusses the extent of testing to be accomplished before production release.

2.13 Logistics Considerations

This section describes the assumptions determining contractor or agency support, initially and over the life of the acquisition, including contractor or agency maintenance and servicing and distribution of commercial items. It also describes the reliability, maintainability, and quality assurance requirements, including any planned use of warranties. It also describes the requirements for contractor data and data rights, their estimated cost, and the use to be made of the data. Moreover, it describes standardization, including the necessity to designate technical equipment as "standard" so that future purchases of the equipment can be made from the same manufacturing source.

2.14 Government-Furnished Property
This section indicates the property to be furnished to contractors, including material and facilities, and discusses associated considerations, such as availability, or the schedule for its acquisition.

2.15 Government-Furnished Information
This section discusses any Government information, such as manuals, drawings, and test data, to be provided to prospective offerors and contractors.

2.16 Environmental and Energy Conservation Objectives
This section discusses all applicable environmental and energy conservation issues associated with the acquisition, the applicability of an environmental assessment or environmental impact statement, the proposed resolution of environmental issues, and any environmentally related requirements to be included in solicitations and contracts.

2.17 Security Considerations
This section discusses, for acquisitions dealing with security-related matters, how adequate security will be established, maintained, and monitored.

2.18 Other Considerations
This section discusses, as applicable, other considerations, such as standardization concepts, the industrial readiness program, the Defense Production Act, the Occupational Safety and Health Act, foreign sales implications, and any other matters germane to the plan and not covered elsewhere.

2.19 Milestones for the Acquisition Cycle
This section addresses the following steps, and any others as appropriate: acquisition plan approval; SOWs; specifications; data requirements; completion of acquisition package preparation; purchase requests; justification and approval for other than full and open competition; issuance of synopsis; issuance of solicitation; evaluation of proposals, audits, and field reports; beginning and completion of negotiations; contract preparation, review, and clearance; and contract award.

2.20 Acquisition Plan Contacts
This section lists the individuals who participated in preparing the acquisition plan, and provides contact information for each.

Exhibit D-1: Sample Acquisition Plan Outline

Configuration Management Plan

The Configuration Management (CM) Plan establishes uniform CM practices in a system development project to manage the establishment of and changes to, system hardware and software. CM helps maintain the integrity of the system throughout its life cycle and facilitates communication about the system among project team members, users, and other supporting organizations. CM guidelines are applied through the systematic identification, control, and auditing of system characteristics, including the following:

- Configuration identification of functional and physical characteristics of a system through structured documentation baselines.
- Configuration control of changes to the physical and functional characteristics of hardware and software systems and the baseline documentation describing them.
- Configuration status accounting about the current configuration and changes to it.
- Configuration auditing to verify that system performance and configuration are accurately identified in the baseline documentation.
- Storage and control of access to the baseline documentation, source code, and executable code.

A baseline is a documented technical description that becomes a reference point against which changes can be proposed, evaluated, and incorporated. A sample outline of a CM Plan is shown in Exhibit D-2.

Sample Configuration Management Plan Outline

Cover Page
Table of Contents

1. Introduction
   Provide a brief statement that introduces the CM plan and describes, in general terms, its use in managing the configuration of the specific projects.

   1.1 Purpose
   Describe why this CM plan was created, what it accomplishes, and how it is used.

   1.2 Scope
   Define the scope of CM planning. Include the Systems Development and Life Cycle Management (SDLCM)) work pattern and its limits, effects of CM on the conduct of development methodology, and effects of the involvement of other contractors within the CM process.

1.3 Policy
Identify policy decisions that affect the conduct of CM on the project.

1.4 System Description
Briefly *describe the system, its history, and the environment in which the project operates (mainframe, client/server, or stand-alone). Describe the system architecture, operating system, and application languages. Identify other legacy or new systems with which this system interfaces. List the number of sites that are using the system.*

1.5 Definitions
Define the terms that appear in the CM plan.

1.6 Reference Documents
List the documents that are referenced to support the CM process including any project or standards documents referenced in the body of the CM plan.

2. Organization
Identify the organization in which CM resides and all organization units that participate in the project. Define the functional roles of these organizational units within the project structure.

2.1 CM Activities
Identify all CM functions required to manage the configuration of the system.

2.2 CM Responsibilities
List CM responsibilities in supporting this project.

3. Configuration Identification
Explain that Configuration Identification is the basis on which the configuration items (CIs) are defined and verified; CIs and documents are labeled; changes are managed; and accountability is maintained.

3.1 Configuration Item Identification
Identify the CIs to be controlled and specify a means of identifying changes to the CIs and related baselines.

3.2 Identification Conventions
Describe the identification (numbering) criteria for the software and hardware structure, and for each document or document set.

3.3 Naming Conventions
Provide details of the file naming convention to be used on the project and how file configuration integrity will be maintained.

3.4 Labels
Describe the requirements for labeling media and application software.

3.5 Configuration Baseline Management
Describe what baselines are to be established. Explain when and how they will be defined and controlled.

3.6 Libraries
Identify the libraries and the media under control, the requirements for the control of

documentation, and how access control is to be managed.

4. Configuration Control
Explain that configuration change management is a process for managing configuration changes and variances in configurations.

4.1 Change Process
Define the process for controlling changes to the system baselines and for tracking the implementation of those changes.

4.2 Review and Control Board(s)
Describe any Internal Review Boards and Configuration Control Boards that will be established for the project. For each board, discuss the members who will participate (and their functional representatives), the Chair, the Secretariat, and the responsibilities of the board and of each member to the board.

4.3 Interface Management
Identify the interfaces to be managed and describe the procedures for identification of interface requirements, establishment of interface agreements, and participation in any Interface Control Working Groups.

5. Configuration Status Accounting
Explain that Configuration Status Accounting (CSA) is the process of keeping records of all change actions pertaining to a configuration item to generate reports on all decisions made and implemented. Also, show that CSA provides a means of storing and cross-referencing the collected data.

6. Configuration Audits
Describe how peer review audits will be accomplished.

7. Reviews
Describe how the technical reviews relate to the establishment of baselines and explain the role of CM in these reviews.

8. CM Plan Maintenance
Describe the activities and responsibilities necessary to ensure continued CM planning during the life cycle of the project; state who is responsible for monitoring the CM plan. Describe how frequently updates are to be performed; how changes to the CM plan are to be evaluated and approved; and how changes to the CM plan are to be made and communicated.

Exhibit D-2: Sample Configuration Management Plan Outline

Preliminary Design Document

The preliminary design document describes the requirements, operating environment, and design characteristics for an information system. It is used in conjunction with the functional requirements document (FRD) to provide a complete system specification of all user requirements for the system and will reflect the user's perspective of the system design. A sample outline for a preliminary design document is provided in Exhibit D-3.

Sample Preliminary Design Document Outline

Cover Page
Table of Contents

1. Introduction
   1.1 Purpose and Scope
   This section provides a brief description of the preliminary design document's purpose and scope.
   1.2 Project Executive Summary
   This section provides a description of the project from a management perspective and an overview of the framework within which the conceptual system design was prepared. If appropriate, include the information discussed in the subsequent sections in the summary.
   1.2.1 System Overview
   This section describes the system in narrative form using non-technical terms. It should provide a high-level system architecture diagram showing a subsystem breakout, if applicable. The high-level system architecture or subsystem diagrams should show interfaces to preliminary systems.
   1.2.2 Design Constraints
   This section describes any constraints in the system design and describes any assumptions made by the project team in developing the system design.
   1.2.3 Future Contingencies
   This section describes any contingencies that might arise in the design of the system.
   1.3 Document Organization
   This section describes the organization of the preliminary design document.
   1.4 Points of Contact
   This section provides the organization code and title of the important points of contact (and alternates if appropriate) for the information system development effort. These points of contact should include the Project Manager, Project Owner and/or Functional Manager, Project User, Quality Assurance (QA) Manager, Security Manager, and Configuration Manager, as appropriate.
   1.5 Project References
   This section provides a bibliography of essential project references and deliverables that have been produced before this point. For example, these references might include the PMP, Feasibility Study, Cost Benefit Analysis, Acquisition Plan, QA plan, Configuration Management Plan, and FRD.
   1.6 Glossary
   This section supplies a glossary of all terms and abbreviations used in the document. If the glossary is several pages in length, it may be included as an appendix.

2. System and Subsystem Specification
   In this section, describe the system and subsystem specifications for the project. Provide a summary of the intended capabilities of the system and subsystems in terms of major components (work flows, process flows, and data models). Add as much detail as necessary to fully define all specifications that will achieve the conceptual system design objectives.
   2.1 System and Subsystem Overview
   This overview supplements the project executive summary with the following technical details: a narrative description of the preliminary conceptual design of the system identified in the project

executive summary with a high-level description of each subsystem; high-level diagrams of each subsystem with more detail (if known at this point) than the diagrams in the project executive summary; a matrix of requirements versus design components

2.2 Specification Model

This section describes the specification model in terms of a workflow, process flow, and data model, if appropriate. Include the data discussed in the subsequent sections.

2.2.1 Workflow

This section provides high-level diagrams identifying the customers' workflow processes among their offices and people at the task level. Identify the automated versus manual processes.

2.2.2 Process Flow

This section provides high-level diagrams that identify the interaction among various organizational functions. Include all primary functional processes as well as any support functions that should be described in the RD. Identify the automated versus manual processes.

2.2.3 Data Model

This section provides high-level documentation regarding the database framework, integration, and divisional models, including descriptions of the database transaction journal capabilities that enable the user to track transactions from original sources to final storage locations.

2.3 Prototypes

Create, use, and evaluate any prototypes to assist in the confirmation or completion of the FRD or act as the deliverable for a particular task or function design within the design phase. The prototype should only be used as a tool for completing the Planning and Requirements Definition and Design phases and should not replace the deliverables from these phases. Prototypes should not be placed into production. Well-developed prototypes may be used for preliminary user training and documentation; however, doing so may require system revisions based on changes to the final system on completion of construction and testing.

3. Traceability (Requirements Traceability Matrix)

In this section, extend the traceability matrix created in the FRD to include features from the preliminary design that address user requirements. This matrix begins with the user requirements and assists in tracing how the requirements are addressed in subsequent phases and documents.

Exhibit D-3: Sample Preliminary Design Document Outline

Detailed Design Document

The Detailed Design Document describes the detailed system and subsystem designs, and detailed requirements that will be used in developing the information system. It contains the database structure, file structures, input formats, output layouts, and module processing logic to be used by the project team during system development. The sections and subsections of the final design document may be organized, rearranged, or repeated as necessary to reflect the best organization for a particular project. A sample outline for a Detailed Design Document is shown is Exhibit D-4.

Sample Detailed Design Document Outline

Cover Page Table of Contents

1. Introduction
   - 1.1 Purpose and Scope
     This section describes the final design document purpose and scope.
   - 1.2 Organization of this Document
     This section describes the organization of the final design document.
   - 1.3 Points of Contact
     Provide the organization and title of the key points of contact (and alternates if appropriate) for the information system development effort in this section. These points of contact should include the Project Manager, Project Owner, system developer, programmer analyst, Quality Assurance (QA) Manager, Security Manager, Configuration Manager, and other points of contact as appropriate.
   - 1.4 Project References
     In this section, provide a bibliography of key project references and deliverables that have been produced before this point. For example, these references might include the Project Management Plan, feasibility study, cost-benefit analysis, acquisition plan, QA plan, Configuration Management Plan, Requirements document (RD), computer security plan, and preliminary design document.
   - 1.5 Glossary
     Supply a glossary of all terms and abbreviations used in this document. If the glossary is several pages in length, it may be included as an appendix.

2. System Design Overview
   This section briefly describes the system and subsystem architectures and their design specifications. The overview information in this section may partially repeat some of the content of the preliminary design document (such as, the system description and the flow diagrams). The content of this section should include the following: a narrative description of the system that describes all system inputs and outputs; a high-level block diagram of the system; forms sequences illustrating the detailed flow of events; object models; database schema; a system data dictionary.

3. Unit Design Organization
   This section describes the segmentation of the system into subsystems (this section may reference the preliminary design document); segmentation of the subsystems into design units (a subsystem may map to one or more design unit per subsystem); and the segmentation of design units into design modules. The section should show - graphically or in tables - the relationship between design modules and the projected actual computer program compilation units. There may be one or more design module per program compilation unit, depending on the software design approach and the computer languages used. The degree and type of modularity above may be modified as necessary for the project under development.

4. File and Database Design
   Interact with the Data Administrator when preparing this section. The section should reveal the final design of all database management system (DBMS) files and the non-DBMS files associated with the system under development in this section. Additional information may be added as required for the particular project.

4.1 Database Management System Files

This section reveals the final design of the DBMS files and includes the following information: final logical design; a physical database description; access methods; estimate of the DBMS file size or volume; and a definition of the update frequency of the database.

4.2 Non-Database Management System Files

In this section, provide the detailed description of all non-DBMS files and include a narrative description of the usage of each file - including whether the file is used for input, output, or both. If this file is a temporary file, include an indication of which modules read and write the file, etc.; and file structures.

5. Input and Output Design

This section provides the detailed design of the system and subsystem inputs and outputs. Any additional information may be added to this section and may be organized according to whatever structure best presents the system input and designs. Depending on the particular nature of the project, it may be appropriate to repeat these sections at both the subsystem and design module levels. Additional information may be added to the subsections if the suggested lists are inadequate to describe the project inputs and outputs.

5.1 System Input Design

This section is a description of the input media used for preliminary data transfers. For example, electronic data interchange, magnetic tape, scanned paper, etc. If appropriate, the input record types, file structures, and database structures provided in Section 4, File and Database Design may be referenced. Define data element definitions. Provide the layout of all input data screens or windows. Provide a graphic representation of each interface. Define or reference all data elements associated with each screen or window.

5.2 System Output Design

This section describes the system output design. System outputs include reports, data display screens, windows, and files. The output files are described in Section 4, and may be either repeated or referenced.

6. Detailed Module Design

A module is the lowest level of design granularity in the system. Depending on the software development approach, there may be one or more modules per program. This section should provide enough detailed information about logic and data necessary to correctly write source code for all modules in the system in this section. At the point at which this document is written, development of the detailed design has been completed for the modules, and that design is documented in this section.

7. Traceability (Requirements Traceability Matrix)

This section extends the traceability matrix created in the FRD to include features from the final design that address user requirements. This matrix begins with the user requirements and assists in tracing how the requirements are addressed in subsequent phases and documents. The matrix may also show traceability between FRD requirements, detailed requirements, and detailed design.

8. System Integrity Controls

Address integrity controls for protecting classified systems and data. This section may reference other documentation.

Appendix A: Detailed system requirements developed from Functional Requirements.

Exhibit D-4: Sample Detailed Design Document Outline

Systems Development and Life Cycle Management (SDLCM)

APPENDIX E – DEVELOPMENT AND TEST PHASE DELIVERABLES

Implementation Plan

The implementation plan describes how the information system will be installed and transitioned into an operational system. The plan contains an overview of the system, a brief description of the major tasks involved in the implementation, the overall resources needed to support the implementation effort (such as hardware, software, facilities, materials, and personnel), and any site-specific implementation requirements. A sample outline for an Implementation Plan is provided in Exhibit E-1. A description of each of the subsections follows.

Sample Implementation Plan Outline

Cover Page
Table of Contents

1. Introduction
   1.1 Purpose
   1.2 System Overview
      1.2.1 System Description
      1.2.2 System Organization
   1.3 Project References
   1.4 Glossary

2. Management Overview
   2.1 Description of Implementation
   2.2 Points of Contact
   2.3 Major Tasks
   2.4 Implementation Schedule
   2.5 Security
      2.5.1 System Security Features
      2.5.2 Security During Implementation

3. Implementation Support
   3.1 Hardware, Software, Facilities, and Materials

3.1.1 Hardware
3.1.2 Software
3.1.3 Facilities
3.1.4 Material
3.2 Personnel
3.2.1 Personnel Requirements and Staffing
3.2.2 Training of Implementation Staff
3.3 Performance Monitoring
3.4 CM Interface

4. Implementation Requirements by Site
4.1 Site Name or Identification for Site X
4.1.1 Site Requirements
4.1.2 Site Implementation Details
4.1.3 Back-Off Plan
4.1.4 Post-implementation Verification

Exhibit E-1: Sample Implementation Plan Outline

A description of each of the sections of the sample Implementation Plan follows.

1. Introduction - This section provides an overview of the information system and includes any additional information that may be appropriate.

1.1 Purpose - This section describes the purpose of the implementation plan. Reference the system name and identify information about the system to be implemented.

1.2 System Overview - This section provides a brief overview of the system to be implemented, including a description of the system and its organization.

1.2.1 System Description - This section provides an overview of the processes the system is intended to support. If the system is a database or an information system, provide a general discussion of the description of the type of data maintained and the operational sources and uses of those data.

1.2.2 System Organization - This section provides a brief description of system structure and the major system components essential to the implementation of the system. It should describe both hardware and software, as appropriate. Charts, diagrams, and graphics may be included.

1.3 Project References - This section provides a bibliography of essential project references and deliverables that have been produced before this point in the project development. For example, these references might include the Project Management Plan, Acquisition Plan, Functional Requirements Document (FRD), Test Plan, conversion plan, and preliminary and final detailed design documents.

1.4 Glossary - Provide a glossary of all terms and abbreviations used in the manual. If it is several pages in length, it may be placed in an appendix.

2. Management Overview - The subsequent sections provide a brief description of the implementation and major tasks involved in this section.

2.1 Description of Implementation - This section provides a brief description of the system and the planned implementation approach.

2.2 Points of Contact - In this section, list all managers and staff with whom the implementation must be coordinated, the name of the responsible organization(s), and titles and telephone numbers of the staff who serve as points of contact for the system implementation. These points of contact could include the System Owner, Project Manager, Security Manager, Database Administrator, Configuration Management Manager, or other managers with responsibilities relating to the system implementation. The site implementation representative for each installation or implementation site should also be included, if appropriate.

2.3 Major Tasks - This section provides a brief description of each major task required for the implementation of the system. Add as many subsections as necessary to this section to describe all the major tasks adequately. The tasks described in this section are not site-specific, but generic or overall project tasks that are required to install hardware and software, prepare data, and verify the system. Include the following information for the description of each major task, if appropriate: what the task will accomplish; resources required to accomplish the task; key person(s) responsible for the task; and criteria for successful completion of the task.

2.4 Implementation Schedule - In this section, provide a schedule of activities to be accomplished during implementation. Show the required tasks (described in Section 2.3, Major Tasks) in chronological order, with the beginning and end dates of each task.

2.5 Security - If appropriate for the system to be implemented, include an overview of the system security features and requirements during the implementation. If the Privacy Act covers the system, provide Privacy Act concerns.

2.5.1 System Security Features - In this section, provide an overview and discussion of the security features that will be associated with the system when it is implemented. It should include the primary security features associated with the system hardware and software. Security and protection of sensitive agency data and information should be discussed, if applicable. Reference the sections of previous deliverables that address system security issues, if appropriate.

2.5.2 Security During Implementation - This section addresses security issues specifically related to the implementation effort, if any. For example, if local area network (LAN) servers or workstations will be installed at a site with sensitive data preloaded on non-removable hard disk drives, address how security would be provided for the data on these devices during shipping, transport, and installation because theft of the devices could compromise the sensitive data.

3. Implementation Support - This section describes the support software, materials, equipment, and facilities required for the implementation, as well as the personnel requirements and training necessary for the implementation. The information provided in this section is not site-specific. If there are additional support requirements not covered by the subsequent sections, others may be added as needed.

3.1 Hardware, Software, Facilities, and Materials - In this section, list support software, materials, equipment, and facilities required for the implementation, if any.

3.1.1 Hardware - This section provides a list of support equipment and includes all hardware used for testing the implementation. For example, if a client/server database is implemented on a LAN, a network monitor or "sniffer" might be used, along with test programs, to determine the performance of the database and LAN at high-utilization rates. If the equipment is site-specific, list it in Section 4, Implementation Requirements by Site.

3.1.2 Software - This section provides a list of software and databases required to support the implementation. Identify the software by name, code, or acronym. Identify which software is commercial off-the-shelf and which is DOL-specific. Identify any software used to facilitate the implementation process. If the software is site-specific, list it in Section 4.

3.1.3 Facilities - In this section, identify the physical facilities and accommodations required during implementation (e.g., physical workspace for assembling and testing hardware components, desk space for software installers, and classroom space for training the implementation staff). Specify the hours per day needed, number of days, and anticipated dates. If the facilities needed are site-specific, provide this information in Section 4.

3.1.4 Material - This section provides a list of required support materials, such as magnetic tapes and disk packs.

3.2 Personnel - This section describes personnel requirements and any known or proposed staffing requirements, if appropriate. Also, describe the training, if any, to be provided for the implementation staff.

3.2.1 Personnel Requirements and Staffing - In this section, describe the number of personnel, length of time needed, types of skills, and skill levels for the staff required during the implementation period. If particular staff members have been selected or proposed for the implementation, identify them and their roles in the implementation.

3.2.2 Training of Implementation Staff - This section addresses the training, if any, necessary to prepare staff for implementing and maintaining the system; it does not address user training, which is the subject of the training plan. Describe the type and amount of training required for each of the following areas for the system: system hardware/software installation; system support; and system maintenance and modification. Present a training curriculum listing the courses that will be provided,

a course sequence, and a proposed schedule. If appropriate, identify which courses particular types of staff should attend by job position description.

3.3 Performance Monitoring - This section describes the performance monitoring tool and techniques and how it will be used to help decide if the implementation is successful.

3.4 CM Interface - This section describes the interactions required with the Configuration Management (CM) representative on CM-related issues, such as when software listings will be distributed, and how to confirm that libraries have been moved from the development to the production environment.

4. Implementation Requirements by Site - This section describes specific implementation requirements and procedures. If these requirements and procedures differ by site, repeat these subsections for each site; if they are the same for each site, or if there is only one implementation site, use these subsections only once.

4.1 Site Name or Identification for Site X - This section provides the name of the specific site or sites to be discussed in the subsequent sections.

4.1.1 Site Requirements - This section defines the requirements that must be met for the orderly implementation of the system and describes the hardware, software, and site-specific facilities requirements for this area. Any site requirements that do not fall into the following three categories and were not described in Section 3, Implementation Support, may be described in this section, or other subsections may be added following Facilities Requirements: hardware requirements; software requirements; data requirements; and Facilities Requirements.

4.1.2 Site Implementation Details - This section addresses the specifics of the implementation for this site. Include a description of the implementation team, schedule, procedures, and database and data updates. This section should also provide information on the following: team; schedule, procedures; database; and Data Update.

4.1.3 Back-Off Plan - This section specifies when to make the go/no go decision and the factors to be included in making the decision. The plan then goes on to provide a detailed list of steps and actions required restoring the site to the original, pre-conversion condition.

4.1.4 Post-Implementation Verification - This section describes the process for reviewing the implementation and deciding if it was successful. It describes how an action item list will be created to rectify any noted discrepancies. It also references the back-off plan for instructions on how to back-out the installation, if, because of the post-implementation verification, a no-go decision is made.

Test Plan

The Test Plan identifies the tasks and activities needed to be performed so that all aspects of the system are adequately tested and that the system can be successfully implemented. It documents the scope, content, methodology, sequence, management of, and responsibilities for test activities. It describes the test activities of the subsystem integration test, the system test, and the acceptance test (including security testing) in progressively higher levels of detail as the system is developed.

The Test Plan provides guidance for the management of test activities, including organization, relationships, and responsibilities. The test case procedures may be included in the Test Plan or in a separate document, depending on system size. The users assist in developing the Test Plan, which describes the nature and extent of tests deemed necessary. This provides a basis for verification of test results and validation of the system. The validation process ensures that the system conforms to the functional requirements in the Functional Requirements Document (FRD) and that other applications or subsystems are not adversely affected. The Test Plan is a dynamic document used for directing the testing of the system throughout the life cycle. A sample outline for a Test Plan is shown in Exhibit E-2. A description of each of the subsections follows.

Sample Test Plan Outline

Cover Page
Table of Contents

1. Purpose

2. Background

3. Scope

4. Glossary

5. Limitations and Traceability
   - 5.1 Limitations
   - 5.2 Traceability (Functional Requirements Traceability Matrix)

6. Test Plans
   - 6.1 Test Levels
     - 6.1.1 Subsystem Integration Test
     - 6.1.2 System Test
     - 6.1.3 User Acceptance Test
     - 6.1.4 Security Test
   - 6.2 Test Environment and Schedules
     - 6.2.1 Software Description
     - 6.2.2 Milestones
     - 6.2.3 Organizations and Locations
     - 6.2.4 Schedule
     - 6.2.5 Resource Requirements
       - 6.2.5.1 Equipment
       - 6.2.5.2 Software

6.2.5.3 Personnel
6.2.6 Testing Material
6.2.7 Test Training
6.2.8 Test Methods and Evaluation
6.2.8.1 Methodology
6.2.8.2 Conditions
6.2.8.3 Test Progression
6.2.8.4 Data Recording
6.2.8.5 Constraints
6.2.8.6 Criteria
6.2.8.7 Data Reduction

7. Test Descriptions
7.1 Test Name (repeat for each test)
7.1.1 Test Description
7.1.2 Control
7.1.3 Inputs
7.1.4 Outputs
7.1.5 Procedures

Exhibit E-2: Sample Test Plan Outline

1. Purpose - In this section, present a clear, concise statement of the purpose of the project test plan and identify the application system being tested by name. Include a summary of the functions of the system and the tests to be performed.

2. Background - This section should provide a brief description of the history and other background leading up to the system development process. Identify the user organization and the location where the testing will be performed. Describe any prior testing, and note results that may affect this testing.

3. Scope - This section describes the projected boundaries of the planned tests. Include a summary of any constraints imposed on the testing, whether they are because of a lack of specialized test equipment, or constraints on time or resources. Describe constraints in detail in Section 5.1, Limitations.

4. Glossary - This section provides a list of all terms and abbreviations used in this document. If the list is several pages in length, it may be placed as an appendix.

5. Limitations and Traceability - This section elaborates on the limitations summarized in Section 3, Scope, and cross-references the functional requirements and detailed specifications to the tests that demonstrate or partially demonstrate that capability.

5.1 Limitations - This section describes limitations imposed on the testing, whether they are because of a lack of specialized test equipment, or constraints on time or resources. Indicate what steps, if any, are being taken to reduce the program risk because of the test limitation(s).

5.2 Traceability (Functional Requirements Traceability Matrix) - This section expands the traceability matrix created in the FRD by including test activities that address user requirements. The intent is to show that the test plan covers all functionality, performance, and other requirements associated with each design element (unit, module, subsystem, and system) in the internal design document.

6. Test Plans - This section describes the levels of tests that take place during development: integration, system, security, and user acceptance tests, and the planning that is needed. The test environment is described in terms of milestones, schedules, and resources needed to support testing.

6.1 Test Levels - This section should include a list of the types of software testing to be performed. List all applicable levels and enter "Not applicable" if a particular level of testing does not apply to the project.

6.1.1 Subsystem Integration Test - This section discusses the tests that examine the subsystems made up of integrated groupings of software units and modules. This is the first level of testing where problem reports are generated; these reports are classified by severity, and their resolution is monitored and reported. Subsystem integration test results (including the test data sets and outputs produced from the tests) may be delivered as part of the final test plan, with the integration test analysis report or as an appendix.

6.1.2 System Test - This section describes the type of testing that determines system compliance with standards and satisfaction of functional and technical requirements when executed on target hardware using simulated operational data files and prepared test data. System documents and training manuals are examined for accuracy, validity, completeness, and usability. During this testing period, software performance, response time, and ability to operate under stressed conditions are tested. External system interfaces are also tested. All findings are recorded in a system test analysis report.

6.1.3 - Acceptance Test - This section describes the tests performed in a non-production environment that mirrors the environment in which the system will be fielded. Every system feature may be tested for correctness and satisfaction of functional requirements. System interoperability, all documentation, system reliability, and the level to which the system meets user requirements are evaluated. Performance tests may be executed to ensure that screen response time, program run time, operator intervention requirements, and overall system operations meet user requirements. Recovery and restart procedures should be evaluated; interfaces to other applications should also be tested.

6.1.4 Security Test - This section discusses the tests that evaluate compliance with system security and integrity requirements. System backup, recovery, security, audit trails, and reconciliation issues are addressed. Include internal controls or application security features mentioned in the context of security testing. Security testing is performed in the operational (production) environment under the

guidance of designated security staff.

6.2 Test Environment and Schedules - This section documents key elements of the test environment, including milestones, schedule, and resource requirements.

6.2.1 Software Description - This section provides a brief description of the inputs, outputs, and functions of the software being tested.

6.2.2 Milestones - This section lists the milestone events and dates for the testing.

6.2.3 Organizations and Locations - This section provides information on the participating organizations and the location where the software will be tested.

6.2.4 Schedule - This section shows the detailed schedule of dates and events for the testing by location. Events should include familiarization, training, test data set generation, and collection, as well as the volume and frequency of the input for testing.

6.2.5 Resource Requirements - This section and associated statements define the resource requirements for the testing.

6.2.5.1 Equipment - This section shows the expected period of use, types, and quantities of equipment needed.

6.2.5.2 Software - This section lists other software needed to support testing that is not part of the software being tested. This should include debugging software and programming aids as well as many current programs to be run in parallel with the new software to ensure accuracy; any drivers or system software to be used in conjunction with the new software to ensure compatibility and integration; and any software required to operate the equipment and record test results.

6.2.5.3 Personnel - This section lists the number of personnel their skill types, and schedules for personnel - from the user, database, Quality Assurance, security, and development groups - who will be involved in the test. Include any special requirements, such as multiple-shift operation or key personnel.

6.2.6 Testing Material - This section lists the materials needed for the test, such as documentation, software to be tested and its medium, test inputs, sample outputs, test control software, and worksheets.

6.2.7 Test Training - This section describes or references the plan for providing training in the use of the software being tested. Specify the types of training, personnel to be trained, and the training staff.

6.2.8 Test Methods and Evaluation - This section documents the test methodologies, conditions,

test progression or sequencing, data recording, constraints, criteria, and data reduction.

6.2.8.1 Methodology - This section describes the general methodology or testing strategy for each type of testing described in this test plan.

6.2.8.2 Conditions - This section specifies the type of input to be used, such as real-time entered test data or canned data for batch runs. It describes the volume and frequency of the input, such as the number of transactions per second tested, etc. Sufficient volumes of test transactions should be used to simulate live stress testing and to incorporate a wide range of valid and invalid conditions. Data values used should simulate live data and test limited conditions.

6.2.8.3 Test Progression - This section describes the manner in which progression is made from one test to another, so the entire cycle is completed.

6.2.8.4 Data Recording - This section describes the method used for recording test results and other information about the testing.

6.2.8.5 Constraints - This section indicates anticipated limitations on the test because of test conditions, such as interfaces, equipment, personnel, and databases.

6.2.8.6 Criteria - This section describes the rules to be used to evaluate test results, such as range of data values used, combinations of input types used, or maximum number of allowable interrupts or halts.

6.2.8.7 Data Reduction - This section describes the techniques that will be used for manipulating the test data into a form suitable for evaluation - such as manual or automated methods - to allow comparison of the results that should be produced to those that are produced.

7. Test Description - This section describes each test to be performed. Tests at each level should include verification of access control and system standards, data security, functionality, and error processing. As various levels of testing (subsystem integration, system, user acceptance testing, and security) are completed and the test results are documented, revisions or increments of the test plan can be delivered. The subsections of this section should be repeated for each test within the project. If there are many tests, place them in an appendix.

7.1 Test Name - This section identifies the test to be performed for the named module, subsystem, or system. Address the criteria discussed in the subsequent sections for each test.

7.1.1 Test Description - Describe the test to be performed. Tests at each level of testing should include those designed to verify data security, access control, and system standards; system/subsystem/unit functionality; and error processing as required.

7.1.2 Control - Describe the test control, such as: manual, semiautomatic, or automatic insertion

of inputs; sequencing of operations; and recording of results.

7.1.3 Inputs - Describe the data input commands used during the test. Provide examples of input data. At the discretion of the Project Manager, input data listings may also be requested in computer readable form for possible future use in regression testing.

7.1.4 Outputs - Describe the output data expected because of the test and any intermediate messages or display screens that may be produced.

7.1.5 Procedures - Specify the systematic procedures to accomplish the test, include test setup, initialization steps, and termination. Also include effectiveness criteria or pass criteria for each test procedure.

Acceptance Test Report

The Acceptance Test Report documents the results of acceptance test activities as defined in the Test Plan. It records results of the tests and presents the capabilities and deficiencies for review, if applicable. Test Problem reports, documenting problems encountered during testing, are included in the Acceptance Test Report, as appropriate. A sample outline for an Acceptance Test Report is shown in Exhibit E-3 followed by description of each of the report subsections. A sample outline for a Test Problem Report is provided in Exhibit E-4.

Sample Acceptance Test Report Outline

Cover Page
Table of Contents

1. Purpose

2. Scope

3. Reference Documents
   - 3.1 Security
   - 3.2 Glossary

4. Test Analysis
   - 4.1 Test Name (repeat for each test)
     - 4.1.1 System Functions
     - 4.1.2 Functional Capability
     - 4.1.3 Performance Capability

5. Software and Hardware Requirements Findings
   - 5.1 Requirement Number and Name (repeat for each test)
     - 5.1.1 Findings
     - 5.1.2 Limitations

6. Summary and Conclusions
   - 6.1 Demonstrated Capabilities
   - 6.2 System Deficiencies
   - 6.3 System Refinements
   - 6.4 Recommendations and Estimates
   - 6.5 Test Problem Report
   - 6.6 Test Analysis Approval Determination Form

Exhibit E-3: Sample Acceptance Test Report Outline

1. Purpose - This section should present a clear, concise statement of the purpose for the Acceptance Test Report.

2. Scope - This section identifies the system tested and the test(s) conducted covered by this report. Provide a brief summary of the project objectives, and identify the Project Owner and users.

3. Reference Documents - This section provides a bibliography of essential project references and deliverables applicable to acceptance testing. These references might include the Functional Requirements Document, User Manual, Operations Manual, Maintenance Manual, Test Plan, and any prior test reports.

3.1 Security - This section describes any security considerations associated with the system being tested, the test analysis, and the data being handled - such as confidentiality requirements, audit trails, access control, and recoverability. Reference those portions of the document that specifically address system security issues, if any.

3.2 Glossary - This section defines all terms and provides a list of abbreviations used in the test analysis report. If the list is several pages in length, it may be placed as an appendix.

4. Test Analysis - This section describes the results of each test performed. It should include verification of access control and system standards, functionality, and error process. Repeat the subsections of this section for each test performed.

4.1 Test Name - The test performed for the specified system is discussed in this section. For each test, provide the subsequent sections.

4.1.1 System Functions - A high-level description of the functions tested and a description of system capabilities designed to satisfy these functions are contained in this section. Each system function should be described separately.

4.1.2 Functional Capability - This section evaluates the performance of each function demonstrated in the test. This section also assesses the manner in which the test environment may

be different from the operational environment and the effect of this difference on functional capabilities.

4.1.3 Performance Capability - This section quantitatively compares the system performance characteristics with the criteria stated in the test plan. The comparison should identify deficiencies, limitations, and constraints detected for each function during testing. If appropriate, a test history or log can be included as an appendix.

5. Software and Hardware Requirements Findings - This section summarizes the test results, organized according to the numbered requirements listed in the Traceability section of the test plan. Each numbered requirement should be described in a separate section. Repeat the subsections of this section for each numbered requirement covered by the test plan.

5.1 Requirement Number and Name - The requirement number provided in the title to this section is the number from the requirements traceability matrix in the Test Plan and the name provided is the requirement's short name.

5.1.1 Findings - This subsection briefly describes the requirement, including the software and hardware capabilities, and states the findings from one or more tests.

5.1.2 Limitations - This subsection describes the range of data values tested, including dynamic and static data, for this requirement and identifies deficiencies, limitations, and constraints detected in the software and hardware during the testing.

6. Summary and Conclusions

6.1 Demonstrated Capabilities - This section provides an overview and summary analysis of the acceptance-testing program. Describe the overall capabilities and deficiencies of the test activity. In cases where tests were intended to demonstrate one or more specific performance requirements, findings should be presented that compare the test results with the performance requirements. Include an assessment of any differences in the test environment versus the operational environment that may have had an effect on the demonstrated capabilities. Provide a statement, based on the results of acceptance testing concerning the adequacy of the system or module to meet overall security requirements.

6.2 System Deficiencies - This section describes acceptance test results showing system deficiencies. Identify all problems by name and number when placed under configuration control. Describe the cumulative or overall effect of all detected deficiencies on the system of module. Generate Test Problem Reports for each deficiency as required (see Exhibit E-4). If the Test Problem Reports are tracked in an automated database, then include reports extracted from the database in an appendix.

6.3 System Refinements - This section itemizes any indicated improvements in system design or

operation based on the results of the test period. Accompanying each improvement or enhancement suggested should be a discussion of the added capability it provides and the effect on the system design. Name and requirement number when placed under configuration control should indicate the improvements.

6.4 Recommendations and Estimates - This section provides a statement describing the overall readiness for system implementation. For each deficiency, address the effect on system performance and design. Include any estimates of time and effort required for correction of each deficiency and any recommendations on the following: the urgency of each correction; parties responsible for corrections; and recommended solution or approach to correcting deficiencies.

6.5 Test Problem Report - This section contains copies of Test Problem Reports (Exhibit E-4) related to the deficiencies found in the test results. Test Problem Reports will vary according to the IT system development project, its scope and complexity, etc.

6.6 Acceptance Test Approval - This section contains one copy of the Acceptance Test Approval (see Exhibit E-5). This form briefly summarizes the perceived readiness for migration of the software. In the case of a user acceptance test, it serves as the user's recommendation for migration to production.

Test Problem Report

Test Problem Report is generated during testing and is attached to the Acceptance Test Report (see Exhibit E-3), as appropriate. A sample outline for a Test Problem Report is shown in Exhibit E-4.

Sample Test Problem Report Outline

TO: _____

FROM: _____

PREPARER/CONTACT: _____ **PHONE:** _____

PROGRAM BEING TESTED: _____

DESCRIPTION OF TEST PROBLEM

A. Expected Results

B. Actual Results

DISPOSITION OF PROBLEM

Action Taken and Date Corrected

Risk Impact if Problem Not Corrected

Changes Required for Existing Documentation

SIGNATURES: _____ _____
Project Manager System Developer

_____ _____
Date Date

Exhibit E-4: Sample Test Problem Report Outline

Acceptance Test Approval

The Acceptance Test Approval is attached to the Acceptance Test Report (see Exhibit E-2), as needed. It confirms that the IT system satisfies the intent of the project and is ready to proceed to implementation. It documents that acceptance test results have been reviewed and acceptance testing successfully completed. A sample outline for an Acceptance Test Approval is shown in Exhibit E-5.

Sample Acceptance Test Approval Outline

DATE: _____

FROM: _____

TO: _____

We have reviewed the test material for the following project request:

TITLE: _____

We recommend:

() a. Full acceptance. No problems encountered.

() b. Full acceptance. The attached Test Analysis Report describes the problems encountered, which are now corrected.

() c. Full implementation with later correction. The attached Test Analysis Report Describes the impact and expected results of this alternative.

() d. Partial implementation. The attached Test Analysis Report describes the impact and expected results of this alternative.

() e. Rejection. The attached Test Analysis Report describes the reasons.

SIGNATURE: _____ _____
Project Manager Date

SIGNATURE: _____ _____
Designated Approval Authority Date

Exhibit E-5: Sample Acceptance Test Approval Outline

Training Plan

The Training Plan outlines the objectives, needs, strategy, and curriculum to be addressed when training users on the new or enhanced information system. The plan presents the activities needed to support the development of training materials, coordination of training schedules, reservation of personnel and facilities, planning for training needs, and other training-related tasks. A sample outline for a Training Plan is shown is Exhibit E-6. A description of each of the sections in the sample plan follows.

Sample Training Plan Outline

Cover Page
Table of Contents

1. Introduction
 1.1 Background and Scope

1.2 Points of Contact
1.3 Document Organization
1.4 Project References
1.5 Security and the Privacy Act
1.6 Glossary

2. Requirements Traceability (optional)

3. Instructional Analysis
3.1 Development Approach
3.2 Issues and Recommendations
3.3 Needs and Skills Analysis

4. Instructional Methods
4.1 Training Methodology
4.2 Training Database
4.3 Testing and Evaluation

5. Training Resources
5.1 Course Administration
5.2 Resources and Facilities
5.3 Schedules
5.4 Future Training

6. Training Curriculum

Exhibit E-6: Sample Training Plan Outline

1. Introduction - This section provides a management summary of the entire plan. It is not required to provide information in this section if the descriptions provided in the subsequent sections are sufficient.

1.1 Background and Scope - This section provides a brief description of the project from a management perspective. It identifies the system, its purpose, and its intended users. This section also provides a high-level summary of the training plan and its scope.

1.2 Points of Contact - This section provides the organization name (code) and the titles of key points-of-contact for system development. It includes such points-of-contact as the Project Manager, QA Manager, Security Manager, Training Coordinator, and Training representative, as appropriate.

1.3 Document Organization - The organization of the training plan is described in this section.

1.4 Project References - This section provides a bibliography of key project references and deliverables that have been produced before this point. For example, these references might include the PMP, FRD, Test Plan, Implementation Plan, and preliminary and detailed design documents.

1.5 Security and the Privacy Act - If applicable, this section provides a brief discussion of the system's security controls and the need for security and protection of sensitive DOL data. If the system handles sensitive or Privacy Act information, information should be included about labeling system outputs as sensitive or Privacy Act-related. In addition, if the Privacy Act protects the system, include a notification of the Privacy Act's civil and criminal penalties for unauthorized use and disclosure of system data.

1.6 Glossary - This section is a glossary of all terms and abbreviations used in the plan. If it is several pages in length, it may be placed as an appendix.

2. Requirements Traceability Matrix (Optional) - If applicable, this section presents a traceability matrix that lists user requirements as documented in the FRD and traces how they are addressed in such documents as preliminary and final design documents, test plans, and training plans. Cross-reference the user requirements and training needs in the appropriate sections of the Training Plan. The requirements matrix may be broken into segments, if appropriate. For example, provide a separate matrix of the training plan sections that trace to particular sections in the Detailed Design Document, preliminary design, FRD, and the Statement of Work.

3. Instructional Analysis

3.1 Development Approach - This section discusses the approach used to develop the course curriculum and ensure quality-training products. This description includes the methodology used to analyze training requirements in terms of performance objectives and to develop course objectives that ensure appropriate instruction for each target group. The topics or subjects on which the training must be conducted should be listed or identified.

3.2 Issues and Recommendations - Any current and foreseeable issues surrounding training are included in this section. Recommendations for resolving each issue and constraints and limitations should also be listed.

3.3 Needs and Skills Analysis - This section describes the target audiences for courses to be developed. Target audiences include technical professionals, user professionals, data entry clerks, clerical staff members, automated data processing (ADP), non-ADP managers, and executives. The tasks that must be taught to meet objectives successfully and the skills that must be learned to accomplish those tasks are described in this section. A matrix may be used to provide this information. In addition, the training needs for each target audience are discussed in this section. If appropriate, this section should discuss needs and courses in terms of staff location groupings, such as headquarters and field offices.

4. Instructional Methods

4.1 Training Methodology - This section describes the training methods to be used in the

proposed courses. These methods should relate to the needs and skills identified in Section 3.3, Needs and Skills Analysis, and should take into account such factors as course objectives, the target audience for a particular course, media characteristics, training setting criteria, and costs. The materials for the chosen training approach (such as course outlines, audiovisual aids, instructor and student guides, student workbooks, examinations, and reference manuals) should be listed or discussed in this section. Sample formats of materials can be included in an appendix, if desired.

4.2 Training Database - If applicable, this section identifies and discusses the training database and how it will be used during computer systems training. It discusses the simulated production data related to various training scenarios and cases developed for instructional purposes. This section also explains how the training database will be developed. If this section is not applicable to the system involved, indicate "Not applicable."

4.3 Testing and Evaluation - This section describes methods used to establish and maintain QA over the curriculum development process. This description should include methods used to test and evaluate training effectiveness, evaluate student progress and performance, and apply comments to modify or enhance the course materials and structure.

5. Training Resources

5.1 Course Administration - This section describes the methods used to administer the training program, including procedures for class enrollment, student release, reporting of academic progress, course completion and certification, monitoring of the training program, training records management, and security, as required.

5.2 Resources and Facilities - This section describes the resources required by both instructors and students for the training, including classroom, training, and laboratory facilities; equipment such as an overhead projector, projection screen, flipchart or visual aids panel with markers, and computer and printer workstations; and materials such as memo pads and pencils, diskettes, viewgraphs, and slides.

5.3 Schedules - This section presents a schedule for implementing the training strategy and indicating responsible parties. Included are key tasks to be completed, such as when to set up training facilities and schedule participants; other activities essential to training; and dates on which those tasks and activities must be finished. This section provides an overview of tasks; deliverables, such as approach and evaluation forms; scheduled versus actual milestones; and estimated efforts, such as the work plan. In the final version of the Training Plan, actual course schedules by location should be included.

5.4 Future Training - This section discusses scheduled training modifications and improvements. This information can include periodic updating of course contents, planned modifications to training environments, retraining of employees, and other predicted changes. Indicate procedures for requesting and developing additional training.

6. Training Curriculum - This section provides descriptions of the components that make up each course. If a large number of courses or modules is described, place these descriptions in an appendix. Subsections of this section, if any, should be created for each course. Each course may comprise one or more modules. A course description should be developed for each module. At a minimum, each course description should include the course/module name; the length of time the course/module will take; the expected class size (minimum, maximum, optimal); the target audience; course objectives; module content/syllabus; specific training resources required, such as devices, aids, equipment, materials, and media to be used; and any special student prerequisites. The course description could also include information on instructor-to student ratio, total number of students to be trained, estimated number of classes, location of classes, and testing methods.

Maintenance Manual

The maintenance manual provides maintenance personnel with the information necessary to maintain the system effectively. The manual provides the definition of the software support environment, the roles and responsibilities of maintenance personnel, and the regular activities essential to the support and maintenance of program modules, job streams, and database structures. In addition to the items identified for inclusion in the maintenance manual, additional information may be provided to facilitate the maintenance and modification of the system. Appendices to document various maintenance procedures, standards, or other essential information may be added to this document as needed. A sample outline for a Maintenance Manual is shown in Exhibit E-7. A description of each of the subsections of the manual follows.

Sample Maintenance Manual Outline

Cover Page
Table of Contents

1. Introduction
   1.1 Purpose
   1.2 Points of Contact
   1.3 Project References
   1.4 Glossary

2. System Description

2.1 System Application
2.2 System Organization
2.3 Security and the Privacy Act
2.4 System Requirements Cross-Reference

3. Support Environment
3.1 Equipment Environment
3.2 Support Software
3.3 Database Characteristics
3.4 Personnel

4. System Maintenance Procedures
4.1 Conventions
4.2 Verification Procedures
4.3 Error Conditions
4.4 Maintenance Software
4.5 Maintenance Procedures

5. Software Unit Maintenance Procedures

Exhibit E-7: Sample Maintenance Manual Outline

1. Introduction - This section provides general reference information regarding the maintenance manual. Whenever appropriate, additional information may be added to this section.

1.1 Purpose - In this section, describe the purpose of the manual and reference the system name and identifying information about the system and its programs.

1.2 Points of Contact - This section identifies the organization(s) responsible for system development, maintenance, and use. This section also identifies points-of-contact (and alternate if appropriate) for the system within each organization.

1.3 Project Reference - This section provides a bibliography of key project references and deliverables produced during the information system development life cycle. If appropriate, reference the Functional Requirements document (FRD), preliminary design, Detailed Design Document, Test Plan, Acceptance Test Report, other system manuals (e.g., Operations Manual), and User Manuals.

1.4 Glossary - Provide a glossary with definitions of all terms, abbreviations, and acronyms used in the manual. If the glossary is several pages in length, place it as an appendix.

2. System Description - The subsequent sections provide an overview of the system to be maintained.

2.1 System Application - This section provides a brief description of the purpose of the system, the functions it performs, and the business processes that the system is intended to support. If the

system is a database or an information system, include a general description of the type of data maintained, and the operational sources and uses of those data.

2.2 System Organization - In this section, provide a brief description of the system structure, major system components, and the functions of each major system component. Include charts, diagrams, and graphics as necessary.

2.3 Security and the Privacy Act - This section provides an overview of the system's security controls and the need for security and protection of sensitive data.

2.4 System Requirements Cross-Reference - This section contains an exhibit that cross-references the detailed system requirements with the preliminary design document, final design document, and test plans. This document, also called a traceability matrix in other documents, assists maintenance personnel by tracing how the user requirements developed in the FRD are met in other products of the life cycle. Because this information is provided in the Detailed Design Document, it may be appropriate to repeat or enhance that information in this section.

3. Support Environment - This section describes the operating and support environment for the system and program(s). Include a discussion of the equipment, support software, database characteristics, and personnel requirements for supporting maintenance of the system and its programs.

3.1 Equipment Environment - This section describes the equipment support environment, including the development, maintenance, and target host computer environments. Describe telecommunications and facility requirements, if any.

3.1.1 Computer Hardware - This section discusses the computer configuration on which the software is hosted and its general characteristics. The section should also identify the specific computer equipment required to support software maintenance if that equipment differs from the host computer. For example, if software development and maintenance are performed on a platform that differs from the target host environment, describe both environments. Describe any miscellaneous computer equipment required in this section, such as hardware probe boards that perform hardware-based monitoring and debugging of software.

3.1.2 Facilities - This section describes the special facility requirements, if any, for system and program maintenance and includes any telecommunications facilities required to test the software.

3.2 Support Software - This section lists all support software such as operating systems, transaction processing systems, and database management systems (DBMSs) as well as software used for the maintenance and testing of the system. Include the appropriate version or release numbers, along with their documentation references, with the support software lists.

3.3 Database Characteristics - This section contains an overview of the nature and content of

each database used by the system. Reference other documents for a detailed description, including the preliminary design and final design documents as appropriate.

3.4 Personnel - This section describes the special skills required for the maintenance personnel. These skills may include knowledge of specific versions of operating systems, transaction processing systems, high-level languages, screen and display generators, DBMSs, testing tools, and computer-aided system engineering tools.

4. System Maintenance Procedures - This section contains information on the procedures necessary for programmers to maintain the software. If the conventions follow standard programming practices and a standards document, that document may be referenced, if it is available to the maintenance team.

4.2 Verification Procedures - This section includes requirements and procedures necessary to check the performance of the system following modification or maintenance of the system's software components. Address the verification of the system-wide correctness and performance. Present, in detail, system-wide testing procedures. Reference the original development test plan if the testing replicates development testing. Describe the types and source(s) of test data in detail.

4.3 Error Conditions - This section describes all system-wide error conditions that may be encountered within the system, including an explanation of the source(s) of each error and recommended methods to correct each error.

4.4 Maintenance Software - This section references any special maintenance software and its supporting documentation used to maintain the system.

4.5 Maintenance Procedure - This section describes systematic, system-wide maintenance procedures, such as procedures for setting up and sequencing inputs for testing. In addition, present standards for documenting modifications to the system.

5. Software Unit Maintenance Procedures - For each software unit within the system, provide the information requested. If the information is identical for each of the software units, it is not necessary to repeat it for each software unit.

Operations Manual

The Operations Manual provides computer control personnel and computer operators with a detailed operational description of the information system and its associated environments. A sample outline for an Operations Manual is shown in Exhibit E-8. A description of each of the subsections in the manual follows.

Sample Operations Manual Outline

Cover Page
Table of Contents

1. General
   1.1 Introduction and Purpose
   1.2 Project References
   1.3 Glossary

2. System Overview
   2.1 System Application
   2.2 System Organization
   2.3 Software Inventory
   2.4 Information Inventory
      2.4.1 Resource Inventory
      2.4.2 Report Inventory
   2.5 Processing Overview
   2.6 Communications Overview
   2.7 Security
   2.8 Privacy Act Warning

3. Description of Runs
   3.1 Run Inventory
   3.2 Run Sequence
   3.3 Diagnostic Procedures
   3.4 Error Messages
   3.5 Run Descriptions
      3.5.1 Control Inputs
      3.5.2 Primary User Contact
      3.5.3 Data Inputs
      3.5.4 Output Reports
      3.5.5 Restart/Recovery Procedures
      3.5.6 Backup Procedures
      3.5.7 Problem Reporting/Escalation Procedure

Exhibit E-8: Sample Operations Manual Outline

1. General

1.1 Introduction and Purpose - Describe the introduction and purpose of the Operations Manual, the name of the system to which it applies, and the type of computer operation.

1.2 Project References - List, as appropriate, the User Manual, Maintenance Manual and other pertinent documentation.

1.3 Glossary - List any definitions or terms unique to this document or computer operation and subject to interpretation by the user of this document.

2. System Overview

2.1 System Application - Provide a brief description of the system, including its purpose and

uses.

2.2 System Organization - Describe the operation of the system by the use of a chart depicting operations and interrelationships.

2.3 Software Inventory - List the software units, to include name, identification, and security considerations. Identify software necessary to resume operation of the system in case of emergency.

2.4 Information Inventory - Provide information about data flies and databases that are produced or referenced by the system.

2.4.1 Resource Inventory - List all permanent files and databases that are referenced, created, or updated by the system.

2.4.2 Report Inventory - List all reports produced by the system. Include report name and the software that generates it.

2.5 Processing Overview - Provide information that is applicable to the processing of the system. Include system restrictions, waivers of operational standards, and interfaces with other systems.

2.6 Communications Overview - Describe the communications functions and process of the system.

2.7 Security - Describe the security considerations associated with the system.

2.8 Privacy Act Warning - Include a Privacy Act warning if the Privacy Act covers the system.

3. Description of Runs

3.1 Run Inventory - List the runs showing the software components, the job control batch file names, run jobs, and purpose of each run if any portion of the system is run in batch mode. For online transaction-based processing, provide an inventory of all software components that must be loaded for the software system to be operational.

3.2 Run Sequence - Provide a schedule of acceptable phasing of the software system into a logical series of operations. If the system is a batch system, provide the execution schedule, which shows, at a minimum, the following: job dependencies; day of week/ month/date for execution; time of day or night (if significant); and expected run time in computer units.

3.3 Diagnostic Procedures - Describe the diagnostic or error-detection features of the system, the purpose of the diagnostic features and the setup and execution procedures for any software

diagnostic procedures.

3.4 Error Messages - List all error codes and messages with operator responses, as appropriate.

3.5 Run Descriptions - Provide detailed information needed to execute system runs. For each run, include the information discussed in the subsequent sections.

3.5.1 Control Inputs - Describe all operator job control inputs; for example, starting the run, selecting run execution options, activating an online or transaction-based system, and running the system through remote devices, if appropriate.

3.5.2 Primary User Contact - Identify the user contacts (and alternate if appropriate) for the system, including the person's name, organization, address, and telephone number.

3.5.3 Data Inputs - Describe the following if data input is required at production time: who is responsible for the source data; format of the data; data validation requirements; and disposition of input source and created data.

3.5.4 Output Reports - Identify the report names, distribution requirements, and any identifying numbers expected to be output from the run. Describe reports to be produced from the system run by other than standard means.

3.5.5 Restart/Recovery Procedures - Provide instructions by which the operator can initiate restart or recovery procedures for the run.

3.5.6 Backup Procedures - Provide instructions by which the operator can initiate backup procedures. Cross reference applicable instructions with procedures in the Contingency Plan.

3.5.7 Problem Reporting/Escalation Procedure - Provide instructions for reporting problems to a point of contact. Include the person's name and telephone numbers (that is, office, home, pager, etc.).

Systems Administration Manual

A systems administration manual serves the purpose of an operations manual in distributed (client/server) applications. A sample outline for a Systems Administration Manual is shown in Exhibit E-9. A description of each of the subsections in the manual follows.

Sample Systems Administration Manual Outline

Cover Page
Table of Contents

1. General
   1.1 Introduction and Purpose
   1.2 Project References
   1.3 Glossary

2. System Overview
   2.1 System Application
   2.2 System Organization
   2.3 Information Inventory
      2.3.1 Resource Inventory
      2.3.2 Report Inventory
   2.4 Processing Overview
   2.5 Communications Overview
   2.6 Security
   2.7 Privacy Act Warning

3. Site Profile(s)
   3.1 Site Location(s)
   3.2 Primary Site

4. Systems Administration
   4.1 User and Group Accounts
      4.1.1 Adding/Deleting Users
      4.1.2 Setting User Permissions
      4.1.3 Adding/Deleting User Groups
   4.2 Server Administration
      4.2.1 Creating Directories
      4.2.2 Building Drive Mappings
   4.3 System Backup Procedures
      4.3.1 Maintenance Schedule
      4.3.2 Off-Site Storage
      4.3.3 Maintenance of Backup Log
   4.4 Printer Support
      4.4.1 Maintenance
      4.4.2 Print Jobs
   4.5 System Maintenance
      4.5.1 Monitoring Performance and System Activity
      4.5.2 Installing Programs and Operating System Updates
      4.5.3 Maintaining Audit Records
      4.5.4 Maintenance Reports
   4.6 Security Procedures
      4.6.1 Issuing IDS and Passwords
      4.6.2 License Agreements
   4.7 Network Maintenance
      4.7.1 LAN Design
      4.7.2Communications Equipment
   4.8 Inventory Management
      4.8.1 Maintaining Hardware and Software Configurations

Exhibit E-9: Sample Systems Administration Manual Outline

1. General

1.1 Introduction and Purpose - This section introduces and describes the purpose of the Systems Administration Manual, the name of the system to which it applies, and the type of computer operation.

1.2 Project References - This section lists, as appropriate, the User Manual, Maintenance Manual, and other pertinent available systems documentation.

1.3 Glossary - This section lists all definitions or terms unique to this document or computer operation and subject to interpretation by the user of this document.

2. System Overview

2.1 System Application - This section provides a brief description of the system, including its purpose and uses.

2.2 System Organization - This section describes the organization of the system by the use of a chart depicting components and their interrelationships.

2.3 Information Inventory - This section provides information about data files, and databases that are produced or referenced by the system.

2.3.1 Resource Inventory - This section lists all permanent files and databases that are referenced, created, or updated by the system.

2.3.2 Report Inventory - This section lists all reports produced by the system, including each report name and the Software that generates it.

2.4 Processing Overview - This section provides information that is applicable to the processing of the system. It includes system restrictions, waivers of operational standards, and interfaces with other systems.

2.5 Communications Overview - This section describes the communications functions and process of the system.

2.6 Security - This section describes the security considerations associated with the system.

2.7 Privacy Act Warning - If the Privacy Act covers the system, then this section provides the appropriate Privacy Act notice and warning.

3. Site Profile(s) - This section contains information pertaining to the site(s) where the application is running. That information includes the information contained in the subsequent sections.

3.1 Site Location(s) - This is the official address(es) of the site(s).

3.2 Primary Site - For the site(s) designated as primary, this section describes the essential personnel names and telephone numbers for the automated data processing site contacts.

4. Systems Administration - This section introduces the responsibilities of the System Administrator, as discussed in the subsequent sections.

4.1 User and Group Accounts - This section introduces topics related to system users.

4.1.1 Adding/Deleting Users - This section describes procedures to create/delete user logins and password accounts.

4.1.2 Setting User Permissions - This section describes procedures to give users/restrict access to certain files.

4.1.3 Adding/Deleting User Groups - This section contains procedures to create/delete user groups.

4.2 Server Administration - This section describes procedures to setup servers, including naming conventions and standards.

4.2.1 Creating Directories - This section describes procedures to create server directories.

4.2.2 Building Drive Mappings - This section describes procedures to create server drive mappings.

4.3 System Backup Procedures - This section describes procedures for regularly scheduled backups of the entire network, including data storage, and the creation and storage of backup logs.

4.3.1 Maintenance Schedule (Daily, Weekly*)* - This section describes documented daily and weekly backup schedules and procedures.

4.3.2 Off-Site Storage Procedures - This section describes the location, schedule, and procedures for off-site storage.

4.3.3 Maintaining Backup Log - This section describes procedures for creating and maintaining backup logs.

4.4 Printer Support - This section discusses procedures for installing, operating, and maintaining printers.

4.4.1 Maintenance (Configurations, Toner, Etc.) - This section describes maintenance contracts, procedures, and equipment information.

4.4.2 Print Jobs (Moving, Deleting, Etc.) - This section describes procedures to monitor, delete, and prioritize print jobs.

4.5 System Maintenance - This section discusses procedures for maintaining the file system.

4.5.1 Monitoring Performance and System Activity - This section contains procedures to monitor system usage, performance, and activity. This may include descriptions of system monitoring tools, the hours of peak demand, a list of system maintenance schedules, etc.

4.5.2 Installing Programs and Operating System Updates - This section includes procedures on how and when to install operating system updates.

4.5.3 Maintaining Audit Records of System Operation - This section describes procedures to setup and monitor system audit trails.

4.5.4 Maintenance Reports - This section includes procedures to create and update maintenance reports.

4.6 Security Procedures - This section describes the process for obtaining identifications (IDs) and passwords. It includes information concerning network access and confidentiality requirements.

4.6.1 Issuing IDs and Passwords - This section describes procedures for issuing IDs and passwords.

4.6.2 License Agreements - This section describes licensing agreements and procedures for ensuring that all licenses are current.

4.7 Network Maintenance - This section describes procedures to maintain and monitor the data

communications network.

4.7.1 LAN Design - This section contains a layout of the network.

4.7.2 Communications Equipment - This section contains a layout of the telecommunications equipment.

4.8 Inventory Management - This section contains a complete hardware and software inventory to include make, model, version numbers, and serial numbers.

4.8.1 Maintaining Hardware and Software Configurations - This section describes procedures for maintaining the configuration information for the hardware and software actually installed.

4.8.2 Maintaining Floor Plans - This section describes procedures for maintaining floor plans showing the location of all installed equipment.

4.8.3 Installing Software/Hardware (New, Upgrades) - This section describes procedures for installing new or upgraded hardware and software.

4.8.4 Maintaining Lists of Serial Numbers - This section describes procedures for maintaining all serial number lists required at a site.

4.8.5 Maintain Property Inventory - This section describes procedures for maintaining a property inventory at the site.

4.9 Training Backup Administrator - This section describes how to train a backup administrator.

4.10 End-User Support Procedures for Support and Contact Information - This section provides necessary end-user contact information and the procedures for providing end-user support.

4.10.1 Escalation Procedures - This section describes the formal escalation procedures to be used by System Administrators in response to priority user problem resolution requests.

4.11 Documentation - This section describes the documentation required of System Administrators as they perform system administration.

4.11.1 Troubleshooting Issues - This section describes how to conduct and document troubleshooting activities.

User Manual

The User Manual contains all essential information for the user to make full use of the information system. This manual includes a description of the system functions and capabilities, contingencies and alternate modes of operation, and systematic procedures for system access and use. Use graphics where possible in this manual. A sample outline for a User Manual is shown in Exhibit E-10. A description of the content of each of the subsections follows.

Sample User Manual Outline

Cover Page
Table of Contents

1. Introduction
   1.1 Purpose and Scope
   1.2 Organization
   1.3 Points of Contact
   1.4 Project References
   1.5 Primary Business Functions
   1.6 Glossary

2. System Capabilities
   2.1 Purpose
   2.2 General Description
   2.3 Privacy Act Considerations

3. Description of System Functions
   3.1 Function X Title
   3.2 Detailed Description of Function
   3.3 Preparation of Function Inputs
   3.4 Results

4. Operating Instructions
   4.1 Initiate Operation
   4.2 Maintain Operation
   4.3 Terminate and Restart Operations

5. Error Handling

6. Help Facilities

Exhibit E-10: Sample User Manual Outline

1. Introduction

1.1 Purpose and Scope - This section provides a description of the purpose and scope of the User Manual.

1.2 Organization - This section describes the organization of the User Manual.

1.3 Points of Contact – This section identifies the organization codes and staff (and alternates if appropriate) who may assist the system user. If a help desk facility or telephone assistance organization exists, describe it in this section.

1.4 Project References - This section provides a bibliography of key project references and deliverables that have been produced before this point in the system development process. References might include the quality assurance plan, Configuration Management Plan, FRD, preliminary design, or Detailed Design Document.

1.5 Primary Business Functions - This section discusses the business perspective of the user's primary responsibilities and tasks as they are supported by the system. Introduce the business functions so that the focus may rest on the systematic steps to support the business functions in later sections.

1.6 Glossary - This section provides a glossary of all terms and abbreviations used in the manual. If the glossary is several pages or more in length, it may be placed as an appendix.

2. System Capabilities - This section provides a brief overview of the system and its capabilities.

2.1 Purpose - This section describes the purpose of the application system.

2.2 General Description - This section provides an overview of the system's capabilities, functions, and operation, including the specific high-level functions performed by the system. Use graphics and tables, if appropriate.

2.3 Privacy Act Considerations

3. Description of System Functions - This section describes each specific function of the system. In this high-level section, describe any conventions to be used in the associated subsections. Each of the subsequent sections should be repeated as often as necessary to describe each function within the system. The term "Function X" in the subsection title is replaced with the name of the function.

3.1 Function X Title - This section provides the title of the specific system function.

3.2 Detailed Description of Function - This section provides a description of each function. Include the following, as appropriate: purpose and uses of the function; initialization of the function, if applicable; execution options associated with this function; description of function inputs; description of expected outputs and results; relationship to other functions; and summary of function operation.

3.3 Preparation of Function Inputs - This section defines required inputs. These inputs should

include the basic data required to operate the system. The definition of the inputs include the following: title of each input; description of the inputs, including graphic depictions of display screens; purpose and use of the inputs; input medium; limitations and restrictions; format and content on inputs, and a descriptive table of all allowable values for the inputs; sequencing of inputs; special instructions; relationship of inputs to outputs; and examples.

3.4 Results - This section describes expected results of the function. Include the following in the description, as applicable: description of results, using graphics, text, and tables; form in which the results will appear; output form and content; report generation; instructions on the use of outputs; restrictions on the use of outputs, such as those mandated by Privacy Act and Computer Security Act restrictions; relationship of outputs to inputs; function-specific error messages; function-specific or context-sensitive help messages associated with this function; and examples.

4. Operating Instructions - This section provides detailed, step-by-step system operating instructions.

4.1 Initiate Operation - This section contains procedures for system logon and system initialization to a known point, such as a system main menu screen. This initialization procedure should describe how to establish the required mode of operation and set any initial parameters required for operation. Software installation procedures should be included if the software is distributed on diskette and should be downloaded before each use.

4.2 Maintain Operation - This section defines procedures to maintain the operation of the software where user intervention is required.

4.3 Terminate and Restart Operations - This section defines procedures for normal and unscheduled termination of the system operations and should define how to restart the system.

5. Error Handling - This section should address error message and help facilities. Additional information and subsections may be added as necessary. Included in this section should be a list of all possible error messages, including the following: any numeric error codes associated with the error message; a description of the meaning of the error message; and a discussion of how to resolve the error.

6. Help Facilities - This section describes any resident help software or any Service or contractors help desk facility that the user can contact for error resolution. Help Desk telephone numbers should be included.

Systems Development and Life Cycle Management (SDLCM)

APPENDIX F – IMPLEMENTATION PHASE DELIVERABLES

Computer Security Certification Package

A security certification refers to the technical evaluation of a system or an application to verify that the installed security safeguards are adequate and work effectively for the system or application. To verify adequacy and effectiveness, these safeguards must be tested. Certification takes place after security tests have been completed and the results of the tests indicate that the system or application meets all applicable policies, regulations, and standards. The Computer Security Certification Package is comprised of 1) a memorandum stating completion of security activities, 2) a Computer Security Certification Statement, 3) a Summary of Compliance, and 4) a Statement of Residual Risk. Exhibits F-1 through F-4 show sample templates for these documents.

Memorandum

Subject: _____ Date: _____
Security Certification

To: _____ From: _____

_____
<DOL Project Manager's Name and Title>

A computer security survey has been conducted on the <system/application name>. A System Security Plan, Security Operating Procedures, and Risk Analysis have been completed that included a review of the security requirements, vulnerabilities, and potential threats against the <system or application>. Based on the results of the risk analysis, identified countermeasures were approved and implemented or planned for implementation.

A Security Test and Evaluation (ST&E) of the <system/application name> was conducted to ensure that implemented countermeasures operate as expected. The results of the ST&E were reviewed and additional countermeasures were planned for implementation if deemed necessary.

The countermeasures that will not be implemented are considered residual risk and are included on the Statement of Residual Risk. Those countermeasures that were implemented after conducting the Risk Analysis and ST&E, and those countermeasures that are planned for implementation in the future, are included on the Summary of Compliance.

A Certification Package for the <system/application name> includes the Sensitive System Worksheet, System Security Plan, Security Operating Procedures, Risk Analysis, Security Test and Evaluation, Summary of Compliance, Statement of Residual Risk, and Certification Statement.

The submission of this memorandum and the attached Certification Package is our commitment to DOL that planned countermeasures will be implemented and based on the findings of our various assessments, our <system or application> is operating at an acceptable level of risk.

Inquiries may be directed to <Security Manager's Name> at <telephone number>.

_____

_____
<DOL Project Manager's Name and Title>

Exhibit F-1: Security Certification Statement Cover Memo

Security Certification Statement

We have carefully considered the security and integrity requirements and the vulnerabilities of the <system/application name>. Based on our review of the requirements, vulnerabilities, potential threats against the applications, and security integrity measures implemented or planned, we have determined that the security capabilities are adequate for known risks. The Statement of Residual Risk is a fair representation of the level of risk remaining for the mainframe applications as of <date>. (See attached sheet)

We have determined that all applicable Federal requirements have been satisfied, and the <system/application name> is operating in the best interest of the Department of Labor. Based on our authority and judgment after weighing the remaining residual risks against operational requirements, we recommend operation (or continued operation) of the applications. We further recommend initiation of the corrective actions listed in the Summary of Compliance to enhance the security and integrity of the <system/application>. (See attached sheet)

Signed: _____
Designated Security Manager

Date: _____

Signed: _____
DOL Project Manager

Date: _____

Exhibit F-2: Sample Security Certification Statement

Summary of Compliance for the _____		
Countermeasure **Note:** List those counter-measures from your Situational Assessment and indicate that you PLAN to implement at your site.	**Actions Needed to Implement Countermeasures**	**Expected Completion Date**
Example: Develop a contingency plan and procedures	**Example:** Identify and document preventative measures that will reduce the effect of potential disasters. Address emergency response, backup, and recovery procedures for each sensitive system.	**Example:** January 3, 2000
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

Exhibit F- 3: Sample Summary of Compliance

Statement of Residual Risk for the _____ Office	
Countermeasure Note: List those countermeasures from your Situational Assessment and indicate that you DO NOT PLAN to implement at your site.	**Reason for Not Implementing the Countermeasure**
Example: Post and maintain an authorized computer room access list.	**Example:** Access to the computer room is provided through an electronic card access device and a unique access code. Access is given to only those personnel who require access to complete their job responsibilities.
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	
12.	

Exhibit F-4: Sample Statement of Residual Risk

Implementation Certification Statement

An implementation certification refers to the technical evaluation of a system or an application to verify that the system to be installed meets all known requirements and that it has been developed and tested in accordance with the provisions in the Project Management Plan and other plans in the systems development life cycle. To verify that the system to be installed meets requirements, the system's features must be tested. Certification takes place after system tests have been completed and the results of the tests indicate that the system or application meets all documented requirements. The Implementation Certification Statement is signed by the System Owner and Project Manager. A sample template is shown in Exhibit F-5.

USER'S CERTIFICATION STATEMENT

I have carefully considered the requirements for the _____ system. Based on reviews of requirements, design documentation, programming, and testing, I have determined that this system conforms to all known requirements and is ready to be installed into production, except for the weaknesses noted in the certification report.

Based upon the report and my judgment, I hereby certify, subject to the corrections recommended in the certification report, that the _____ system meets all documented and approved requirements.

Weighing the remaining residual risks against operational requirements, I recommend that the _____ system be accredited for continued operation and that the recommendations included in the certification report be implemented.

Signed _____ Date _____
Project Manager

I am in concurrence with the above and formally accept the _____ system.

Signed _____ Date _____
System Owner

Exhibit F-5: Sample Implementation Certification Statement

Systems Development and Life Cycle Management (SDLCM)

APPENDIX G – OPERATIONS AND MAINTENANCE PHASE DELIVERABLES

Disposition Plan

The disposition plan is the most significant deliverable in the disposition of the information system, and the plan will vary according to the system and DOL requirements. The objectives of the plan are to end the operation or the system in a planned, orderly manner and to ensure that system components (i.e., hardware, software, data, and documentation) are properly archived or incorporated into other systems. At the end of this task, the system will no longer exist as an independent entity. The completion of the systems life cycle is carefully planned and documented to avoid disruption to the organizations using the system or the operation of other systems that use the data and/or software of the present system. A sample template for a Disposition Plan is provided in Exhibit G-1. A description of the contents of each subsection of the plan follows.

Sample Disposition Plan Outline

Cover Page
Table of Contents

1. Introduction
   - 1.1 Purpose and Scope
   - 1.2 Points of Contact
   - 1.3 Project References
   - 1.4 Glossary

2. System Disposition
   - 2.1 Notifications
   - 2.2 Data Disposition
   - 2.3 Software Disposition
   - 2.4 System Documentation Disposition
   - 2.5 Equipment Disposition

3. Project Closedown
   - 3.1 Project Staff
   - 3.2 Project Records
   - 3.3 Facilities

Exhibit G-1: Sample Disposition Plan Outline

1. Introduction - This section provides a brief description of introductory material.

1.1 Purpose and Scope - This section describes the purpose and scope of the Disposition Plan. Reference the information system name and provide identifying information about the system-undergoing disposition.

1.2 Points of Contact - This section identifies the System Owner. Provide the name of the responsible organization and staff (and alternates, if appropriate) who serve as points of contact for the system disposition. Include telephone numbers of key staff and organizations.

1.3 Project References - This section provides a bibliography of key project references and deliverables that have been produced before this point in the project development. These documents may have been produced in a previous engineering life cycle that resulted in the initial version of the system now undergoing disposition or may have been produced in subsequent enhancement efforts.

1.4 Glossary - This section contains a glossary of all terms and abbreviations used in the plan. If it is several pages in length, it may be placed in an appendix.

2. System Disposition

2.1 Notifications - This section describes the plan for notifying known users of the system being shut down, as well as other affected parties, like those responsible for other interfacing systems and operations staff members involved in running the system.

2.2 Data Disposition - This section describes the plan for archiving, deleting, or transferring to other systems the data files and related documentation in the system being shut down.

2.3 Software Disposition - This section describes the plan for archiving, deleting, or transferring to other systems the software library files and related documentation in the system being shut down.

2.4 System Documentation Disposition - This section describes the plan for archiving, deleting, or transferring to other systems the hardcopy and softcopy systems and user documentation for the system being shut down.

2.5 Equipment Disposition - This section describes the plan for archiving, deleting, or transferring to other systems the hardware and other equipment used by the system being shut down.

3. Project Closedown

3.1 Project Staff - This section describes the plan for notifying project team members of the shutdown of the system, and the transfer of these team members to other projects.

3.2 Project Records - This section describes the plan for archiving, deleting, or transferring to other projects the records of project activity for the project that has been maintaining the system being shut down.

3.3 Facilities - This section describes the plan for transferring or disposing of facilities used by the project staff for the system being shut down.

Systems Development and Life Cycle Management (SDLCM)

APPENDIX H – SDLCM DELIVERABLES MATRIX

Deliverable	Type	Supporting Documents
Conceptual Planning Phase		
Request for Information Technology Services (RITS)/Statement Of Concept	Core	FIPS PUB 64 1.3.1
Cost Benefit Analysis	Core	OMB A-130:Appx IV 8b1; OMB A-94: Section 5; IEEE/EIA 12207.0-1996 Section 5.1.1.6, Clinger-Cohen Act 1996 Sec 5112(c); FIPS PUB 64 1.3.3
Risk Management Plan	Core	OMB Director's Policy Memorandum M-97-02 (Raines Rules); IEEE/EIA 12207.0-1996 Section 5.1.1.6; NIST Handbook March 16, 1995; OMB A-130 Appx III B; IEEE/EIA 12207.2-1997 Section 7.1.2.1 (f)/Annex L, Clinger-Cohen Act 1996 Sec 5112 (a)(b)(c); 5122(a)(b)(5)
Project Management Plan	Core	IEEE/EIA 12207.2-1997 Sec 5.2.4.2
Feasibility Study (s)	Optional	Clinger-Cohen Act 1996 Sec 5122(b)/Sec 5123 ; OMB A-130 Appx IV Sec 8b(1) ; IEEE/EIA 12207.0-1996 Sec 7.1.1.2; FIPS PUB 64 1.3.2
Acquisition Strategy	Optional	See Design Phase
Work Breakdown Structure	Optional	See Design Phase
Statement of Work	Optional	Clinger-Cohen Act 1996 Sec 5312 (c)(2)
Planning and Requirements Definition Phase		
Functional Requirements Document	Core	IEEE/EIA 12207.0-1996 Sec 5.1.1.2/5.1.1.8/5.2.4.3
Project Risk Assessment	Core	OMB A-130 Appx III A 3 a 2 ; OMB A-130 Appx III A 4 a 3) ; OMB A-130 Appx III B a 2 ; OMB A-130 Appx III B a 3 ; NIST Special Publication 500-223 ; FIPS Pub 102 Sec 1.5.1 ; IEEE/EIA 12207.0-1996 Sec 5.1.1.6 ; Clinger-Cohen Act 1996 Sec 5131 (2)(D); IEEE/EIA 12207.0-1996 Sec. 5.2.4.5
System Security Plan/Security Risk Assessment	Core	OMB A-130 Sec 8 Policy-Info Mgmt/Safeguards; OMB A-130 Appx III B a 2) Security plan; IEEE/EIA 12207.0-1996 Sec 5.2.4.5 (l), Clinger-Cohen Section 5131, DOL Computer Security Handbook
Acquisition Plan/Strategy	Optional	See Design Phase
Work Breakdown Structure	Optional	See Design Phase
Configuration Management Plan	Optional	See Design Phase
Test Plan	Optional	See Development and Test Phase
Legacy Data Plan	Optional	IEEE/EIA 12207.2-1997 Sec 5.5.5
Project Management Plan	Update	See Conceptual Planning Phase
Cost Benefit Analysis	Update	See Conceptual Planning Phase
Risk Management Plan	Update	See Conceptual Planning Phase
Design Phase		
Work Breakdown Structure	Core	IEEE/EIA 12207.2-1997 Sec 5.2.4.5 (c)
Configuration Management Plan	Core	IEEE/EIA 12207.2-1997 Sec 6.2/ISO 10007 ; IEEE/EIA 12207.0-1996 Sec 5.2.4.5

Deliverable	Type	Supporting Documents
Detailed Design	Core	IEEE/EIA 12207.2-1997 Sec 5.3.4.2, 5.3.5.6, 5.3.7.5, 5.3.8.5; NIST SP 500-223 Sec 2.2, 2.3
Acquisition Plan Strategy	Core	OMB Memorandum M-97-02 (Raines Rules) ; Clinger-Cohen Act 1996 Sec 5124 ; OMB A-130 Appx IV Sec 8 b(5) ; OMB A-109; IEEE/EIA 12207.0-1996 Sec 5.1.1.2/5.1.1.8/5.2.4
Contingency Plan	Optional	OMB A-130 Appendix III A 3 b 2) d
Implementation Plan	Optional	See Development and Test Phase
Test Plan	Optional	See Development and Test Phase
Project Risk Assessment	Update	See Planning and Requirements Definition Phase; OMB A-130 Sec 8 and Appendix III Ba2; IEEE/EIA 12207.0-1996 Sec 5.2.4.5; Clinger-Cohen Act 1996 Sec 5131.
System Security Plan/Security Risk Assessment	Update	See Planning and Requirements Definition Phase
Project Management Plan	Update	See Conceptual Planning Phase
Cost Benefit Analysis	Update	See Conceptual Planning Phase
Risk Management Plan	Update	See Conceptual Planning Phase
Development and Test Phase		
Test Plan	Core	IEEE/EIA 12207.2-1997 Annex D-H.4 (c),
Acceptance Test Plan	Core	IEEE/EIA 12207.2-1997 Sec 5.3.13.1 and Annex D-H.4
Acceptance Test Report	Core	IEEE/EIA 12207.2-1997 Sec 5.3.13.1/5.3.11.2; IEEE 12207.0-1996 Annex E 3, 4
Acceptance Test Approval	Core	IEEE/EIA 12207.2-1997 Sec 5.3.13.1 and Annex D-H4.
Implementation Plan	Core	IEEE/EIA 12207.2-1997 Sec 5.3.1
System manuals	Core	IEEE/EIA 12207.2-1997 Sec 6.1
User Manuals	Core	IEEE/EIA 12207.2-1997 Sec 6.1
Training Plan	Core	IEEE/EIA 12207.0-1997 Sec 7.4.1.1;OMB A-130 Appendix III A 3a2)b); Clinger-Cohen Act 1996 Section 5112(i) ; IEEE/EIA 12207.0-1996 Sec 5.2.4.5(o)
Delivered System	Core	IEEE/EIA 12207.2-1997 Sec 5.3.12; OMB A-130 Appendix III A
System Fielding Authorization	Optional	IEEE/EIA 12207.2-1997 Sec 5.3.12; NIST Special Pubs 500-223 Sec 2.5
Project Risk Assessment	Update	See Planning and Requirements Definition Phase
Work Breakdown Structure	Update	See Design Phase
Acquisition Plan/Strategy	Update	See Design Phase
System Security Plan/Security Risk Assessment	Update	See Planning and Requirements Definition Phase
Project Management Plan	Update	See Conceptual Planning Phase
Risk Management Plan	Update	See Conceptual Planning Phase
Implementation Phase		
Computer Security Certification	Core	FIPS Pub 102
Security Accreditation Letter	Core	IEEE/EIA 12207.0-1996 Sec 5.3.13; FIPS Pub 102 Sec 2.5.2, 2.6.2; DOL Computer Security Handbook
Implemented System	Core	IEEE/EIA 12207.0-1996 Sec 6.2
Trained Personnel	Core	IEEE/EIA 12207.0-1996 Sec 5.3.13.3 and Sec 5.2.4.5; IEEE/EIA 12207.0-1996 Sec 7.4 ; OMB A-130 Appendix III
Implementation Certification Statement	Core	IEEE/EIA 12207.0-1996 Section 5.3.12
System Security Plan/Security Risk Assessment	Update	See Planning and Requirements Definition Phase
Configuration Management Plan	Update	See Design Phase
User Manuals	Update	See Development and Test Phase
System Manuals	Update	See Development and Test Phase
Project Risk Assessment	Update	See Planning and Requirements Definition Phase
Work Breakdown Structure	Update	See Design Phase
Acquisition Plan/Strategy	Update	See Design Phase

Deliverable	Type	Supporting Documents
Project Management Plan	Update	See Conceptual Planning Phase
Risk Management Plan	Update	See Conceptual Planning Phase
Operations and Maintenance Phase		
Disposition Plan	Core	IEEE/EIA 12207.0-1996 Sec 5.2.4
User Manuals	Update	See Development and Test Phase
System Manuals	Update	See Development and Test Phase
Project Risk Assessment	Update	**See Planning and Requirements Definition Phase**
Risk Management Plan	Update	See Conceptual Planning Phase
System Security Plan/System Risk Assessment	Update	See Planning and Requirements Definition Phase
Disposition Phase		
Archived System	Core	IEEE/EIA 12207.2-1997 Sec 5.5.6.1(b)

Deliverable Types:		
	Core	deliverable is required for this phase
	Optional	deliverable may or may not be produced for this phase
	Update	deliverable may be updated in this phase

Exhibit H-1: SDLCM Deliverables Matrix